



# UFED Logical Analyzer

## User Manual

December 2014



# Legal Notices

Copyright © 2014 Cellebrite Mobile Synchronization Ltd. All rights reserved.

This manual is delivered subject to the following conditions and restrictions:

- This manual contains proprietary information belonging to Cellebrite Mobile Synchronization Ltd. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of the UFED Logical Analyzer.
- No part of this content may be used for any other purpose, disclosed to any person or firm, or reproduced by any means, electronic or mechanical, without the express prior written permission of Cellebrite Ltd.
- The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.

# Contents

## Chapter 1: Introduction ..... 7

## Chapter 2: Installation and activation ..... 9

### 2.1. Installing UFED Logical Analyzer ..... 10

#### 2.1.1. System requirements ..... 10

#### 2.1.2. Software installation..... 11

#### 2.1.3. Activating UFED Logical Analyzer..... 19

#### 2.1.4. Moving UFED Logical Analyzer with a software license to another PC ..... 26

#### 2.1.5. Enabling connectivity with Windows Vista ..... 27

## Chapter 3: Getting started ..... 29

### 3.1. Start UFED Logical Analyzer ..... 29

### 3.2. Opening a file for analysis..... 30

### 3.3. Extracting data to PC ..... 32

### 3.4. Saving a project session..... 39

### 3.5. Loading a project session..... 40

### 3.6. Closing a project..... 41

### 3.7. Closing UFED Logical Analyzer ..... 41

### 3.8. Keyboard shortcuts ..... 42

## Chapter 4: Orientation to the workspace ... 43

### 4.1. Project tree ..... 44

#### 4.1.1. Working in the project tree area..... 52

### 4.2. Data display area..... 53

#### 4.2.1. Welcome tab..... 55

#### 4.2.2. Extraction summary tab..... 57

#### 4.2.3. Data tabs ..... 59

### 4.3. Viewing image files ..... 67

### 4.4. Playing video files..... 68

## Chapter 5: Locating and analyzing information ..... 69

### 5.1. Searching for information in a data tab ..... 69

5.2. Using the quick filter .....	69
5.3. Using the advanced filter .....	72
5.4. Searching for information in all open projects.....	73
5.5. Timeline view.....	74
5.6. Accessing conversation view.....	77
5.7. Working with watch lists .....	79
5.7.1. Creating a watch list.....	80
5.7.2. Editing a watch list.....	83
5.7.3. Importing a watch list .....	84
5.7.4. Exporting a watch list.....	85
5.7.5. Deleting a watch list.....	87
5.7.6. Running a watch list.....	88
5.8. Bookmarking information (entity bookmarks) .....	90
5.8.1. Creating a new entity bookmark.....	91
5.8.2. Editing an entity bookmark .....	92
5.8.3. Deleting an entity bookmark.....	92

## **Chapter 6: Translating decoded data ..... 93**

6.1. Using the feature.....	94
6.2. Updating your license with the selected languages .....	94
6.2.1. Selecting languages in MyCellebrite .....	95
6.2.2. Downloading the translation pack .....	100
6.2.3. Translating the decoded data .....	102
6.2.4. Reporting .....	104

## **Chapter 7: Working with project analytics..... 107**

## **Chapter 8: Scanning for malware ..... 109**

8.1. Updating the signature database (online) .....	110
8.2. Updating the signature database from file (offline).....	112

## **Chapter 9: Generating a report ..... 119**

## **Chapter 10: Performing extractions ..... 131**

10.1. Performing advanced logical extraction.....	131
---	-----

10.1.1. Performing advanced logical extraction.....	132
---	-----

## **Chapter 11: Camera and screenshot evidence.....143**

## **Chapter 12: Settings.....147**

12.1. General settings .....	148
12.2. Data files.....	151
12.2.1. Data files filtering methods.....	153
12.2.2. Managing data files settings.....	154
12.3. Additional report fields .....	157
12.3.1. Adding a new report field.....	158
12.3.2. Deleting a report field .....	160
12.3.3. Editing a report field.....	160
12.4. Report defaults.....	161
12.5. Saving settings.....	169
12.6. Loading settings .....	169
12.7. Setting project settings.....	169

12.7.1. Setting a unified time zone for the project .....	170
12.7.2. Setting the case information.....	173

## **Chapter 13: Reference .....177**

13.1. File menu.....	177
13.2. View menu.....	177
13.2.1. Viewing the trace window .....	178
13.3. Tools menu.....	179
13.4. Extract menu .....	180
13.5. Report menu .....	180
13.6. Help menu .....	183

# Chapter 1: Introduction

Welcome to UFED Logical Analyzer. UFED Logical Analyzer is an application that reads UFED files (UFED dump files \*.ufd) and UFED report (\*.xml) files created as part of the logical extraction and UFED report package (\*.ufdr) generated from analyzed data of a logical extraction by UFED Logical Analyzer.

UFED Logical is made up of two components:

- The UFED device with Logical modules, used to create logical extraction from mobile devices or SIM cards, which can then be saved to a USB disk drive, SD memory card, or directly to your PC.
- UFED Logical Analyzer application, which enables investigators to perform in depth analysis of data extracted as part of a logical extraction.

The UFED Logical workflow consists of two steps:

- Logical extraction using the UFED hardware
- Analysis and reporting using UFED Logical Analyzer

UFED Logical Analyzer enables you to open UFED reports, perform your own search and analysis on the analyzed information, and perform actions such as search, generate reports, create entity bookmarks, and more.





## Chapter 2: Installation and activation

This chapter describes the installation and activation process of UFED Logical Analyzer on your PC.

## 2.1. Installing UFED Logical Analyzer

### 2.1.1. System requirements

PC	Windows compatible PC with a Pentium® IV or compatible processor running at 1.6 GHz or higher		
Operating System	Microsoft Windows XP <sup>1</sup> with SP3 or later Microsoft Windows Vista™, Windows 7 or Windows 8		
Memory (RAM)	OS	Recommended	Minimum
	32 bit	4GB	4GB
	64 bit	8GB	4GB
Space requirements	500 MB of free disk space for installation		
Additional requirements	Microsoft® .Net version 4.0 NOTE: Windows XP 64 bit requires installation of a .Net 2.0 hotfix (NDP20-KB913384-X64.exe) from <a href="http://archive.msdn.microsoft.com/KB913384/Release/ProjectReleases.aspx?ReleaseId=771">http://archive.msdn.microsoft.com/KB913384/Release/ProjectReleases.aspx?ReleaseId=771</a>		

---

<sup>1</sup> By February 28, 2015, the UFED Series will no longer support Windows XP.

Permissions	If you intend to activate the application using a hardware license key (dongle) provided by Cellebrite, you must have administrative rights over the computer.
-------------	--

NOTE: To enable extraction to a PC with Windows Vista Operating System, follow the procedure in *Enabling connectivity with Windows Vista* (page 27).

## 2.1.2. Software installation

### 2.1.2.1. Obtaining a copy of UFED Logical Analyzer

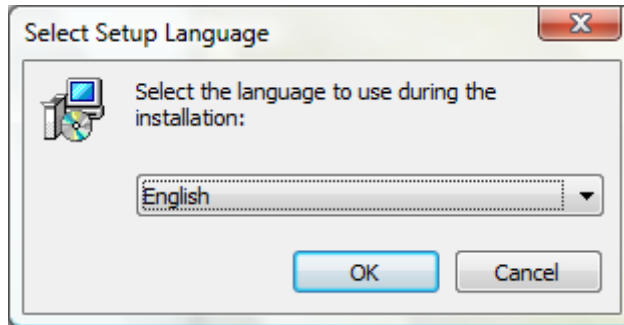
A copy of the latest UFED Logical Analyzer application installer can be obtained from the following sources:

- Downloaded from the MyCellebrite site.
- Downloaded from the link provided in the release notes.

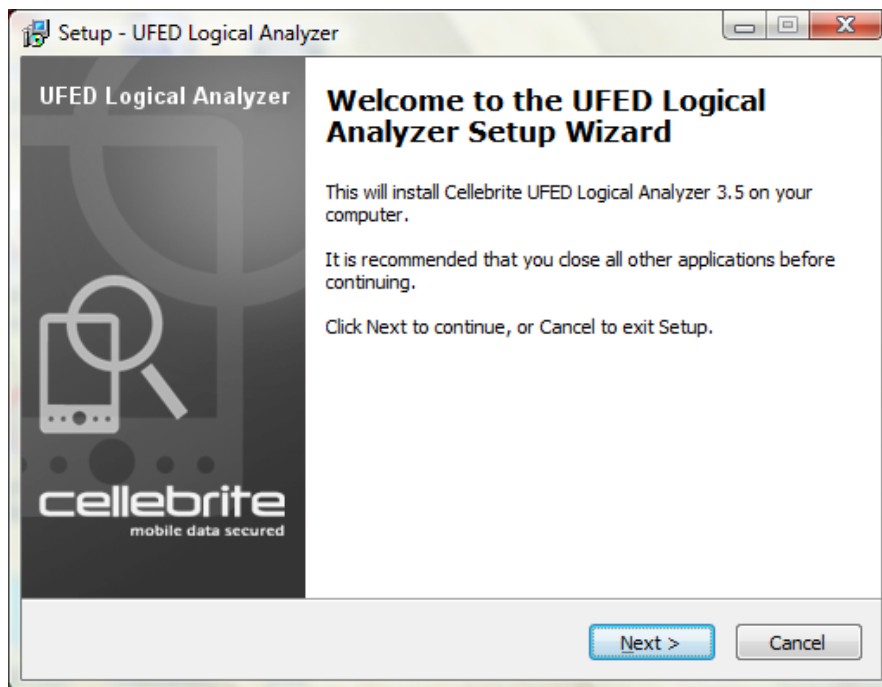
### 2.1.2.2. Installing UFED Logical Analyzer

NOTE: Before you begin, ensure that cable U-441 is not attached to your computer.

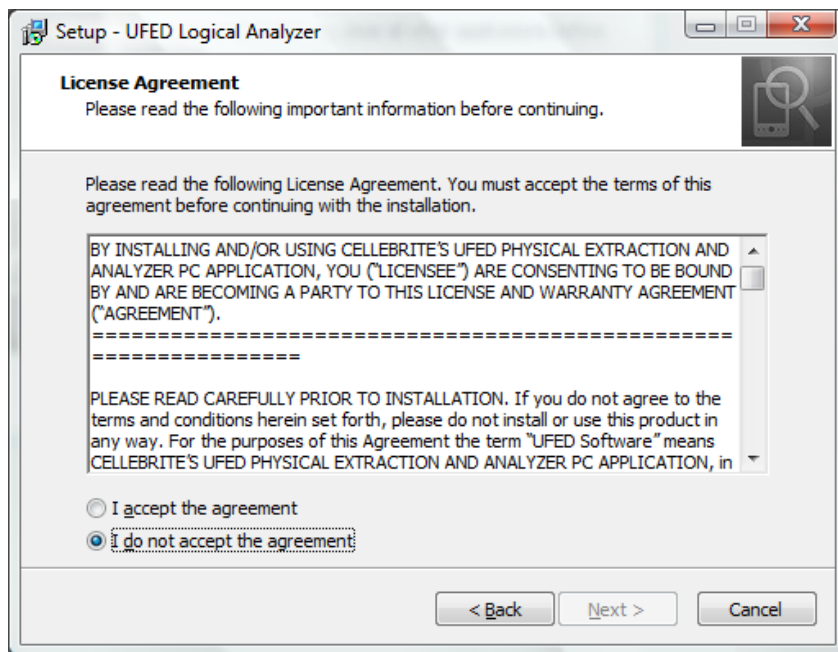
- 1) Double-click the setup file.



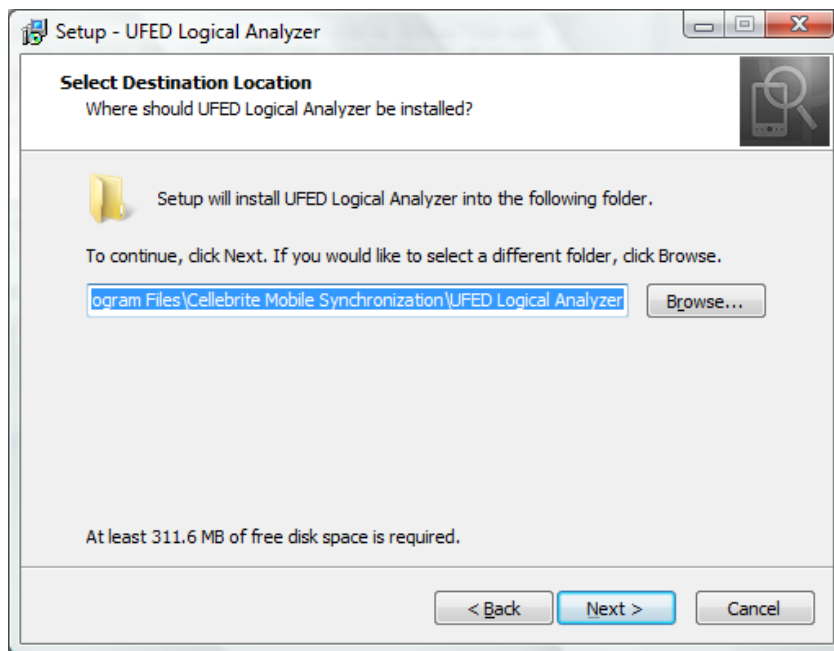
- 2) Select the desired language and click **OK** to continue.



3) Click **Next**.

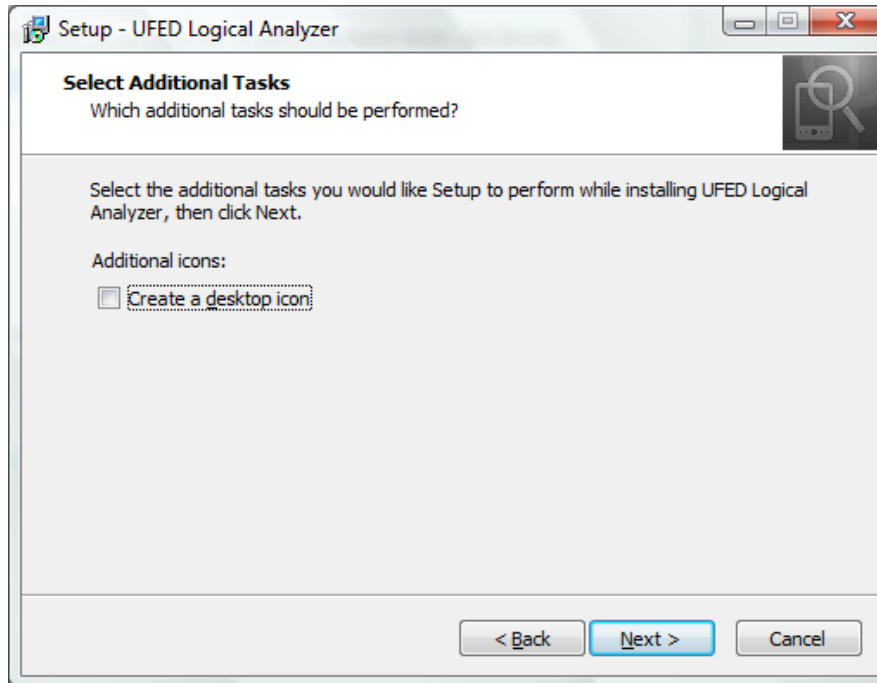


- 4) Select **I accept the agreement**, and click **Next**.



- 5) If desired, click **Browse** and set a different installation folder.

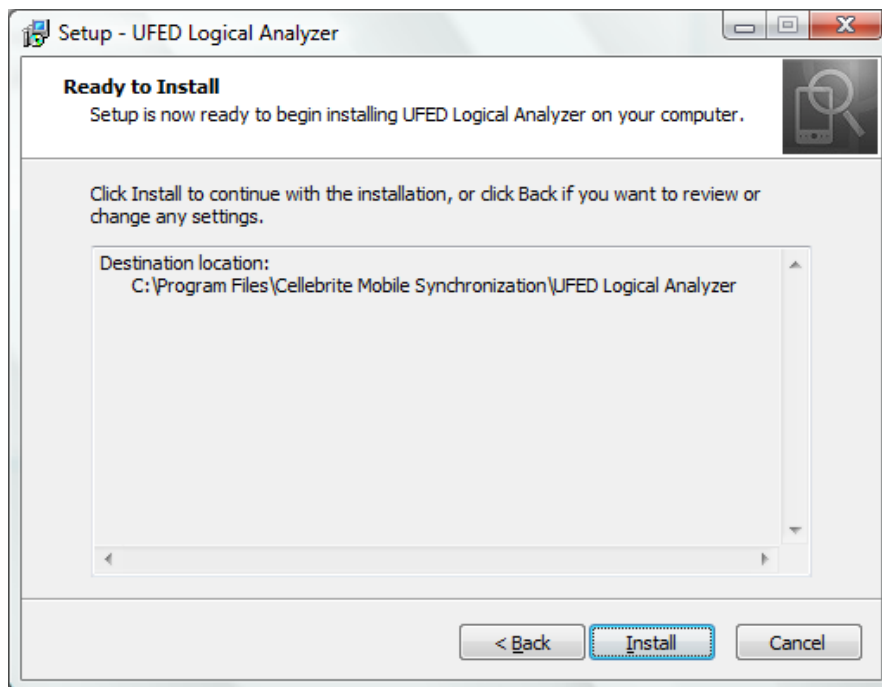
6) Click **Next**.



7) If you do not want a desktop icon, clear the **Create a desktop icon** checkbox.

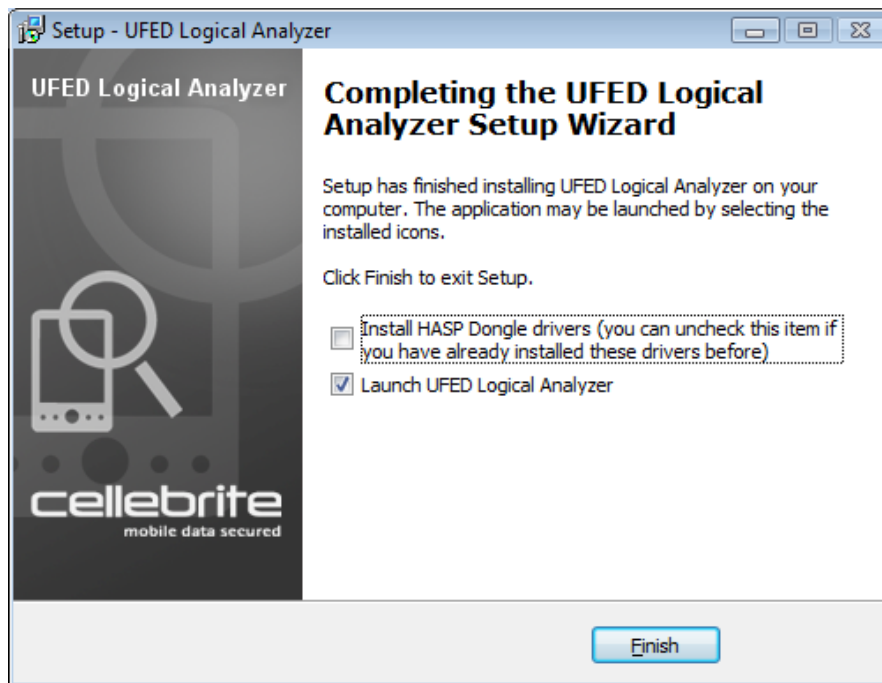


8) Click **Next**.



9) Click **Install**. The installation begins.

**NOTE:** As part of the installation process, you may be prompted to enable download and installing of the Microsoft .NET 3.5 Framework. This installation requires that your computer has Internet access.



- 10) If you intend to activate the application using a hardware license key (dongle) provided by Cellebrite, select **Install Hasp Dongle Drivers**.

**NOTE:** You must have administrative rights to install the HASP dongle drivers.

- 11) To start UFED Logical Analyzer at the end of the installation, select **Launch UFED Logical Analyzer**.
- 12) Click **Finish**.

### 2.1.3. Activating UFED Logical Analyzer

Activate UFED Logical Analyzer in one of the following ways:

- Using a license dongle
- Using a software license
- Using a network dongle

#### 2.1.3.1. New version notification

Cellebrite will inform you when a newer version of your software is available. If you are connected to the internet you will receive this notification when the new version is available. If you are not connected to the internet the notification will appear every 3 months.

### 2.1.3.2. Using a license dongle

Use the UFED dongle provided with your UFED kit. The dongle contains licenses for all the applications purchased.

#### To use UFED Logical Analyzer with a dongle:

- 1) Connect the dongle to a USB port on your computer. The license is automatically located. When the dongle is recognized by the operating system, the application can read the license.
- 2) Start UFED Logical Analyzer.

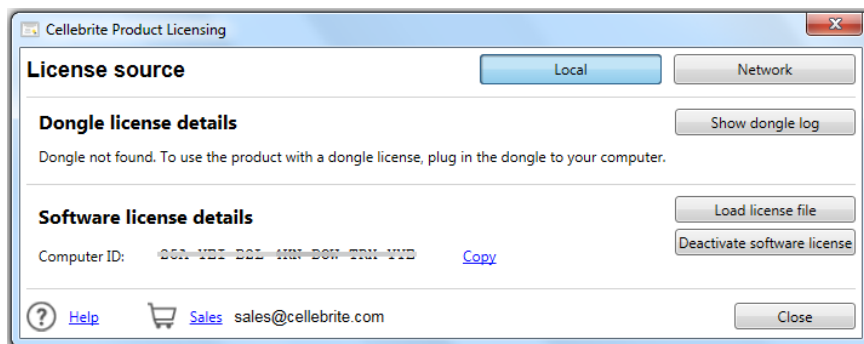
**Congratulations, your application is now ready!**

#### If a license dongle is not found:

- 1) When starting for the first time, or when a license dongle is not found, the Cellebrite Product Licensing window appears.



UFED Dongle



- 2) If you connected the dongle to a USB port on your computer, and it still does not work, contact [support@cellebrite.com](mailto:support@cellebrite.com).

**NOTE:** The HASP dongle drivers must be installed in order to use a hardware license key. If the drivers were not installed during the UFED software installation process, you can run the installation process again and select Install Hasp Dongle Drivers at the end of the process.

### 2.1.3.3. Using the application with a software license

The first time you open the application, you must activate the license.

To use UFED Logical Analyzer with a software license:

- 1) Go to the following link: <https://my.cellebrite.com/logicalanalyzer>
- 2) Sign into your MyCellebrite account.

(If you don't have an account, click **Register now**, create a user, and then go back to the required UFED application link.)

You will be directed to the product activation window.

- 3) Click to download the application and save the file to a PC.
- 4) Extract the zip file, click the installation file and install the software using the Setup Wizard. Restart the PC if required.
- 5) Repeat step 1 to go to the application link.
- 6) In the Activation method box, if you purchased UFED 4PC, select **Activation code** or if you purchased UFED Touch, select **UFED Touch/UFED Classic**.

Activation Method      Activation Code ▼

Activation Method      UFED Touch/UFED Classic ▼

- 7) Depending on the product you purchased, continue as follows:

- **UFED 4PC:** In the Activation Code field, enter the Activation code provided with the UFED 4PC kit.

Activation Code

- **UFED Touch:** In the Choose Serial Number field, select the UFED serial number displayed on the UFED Touch unit or UFED Touch License Activation screen.

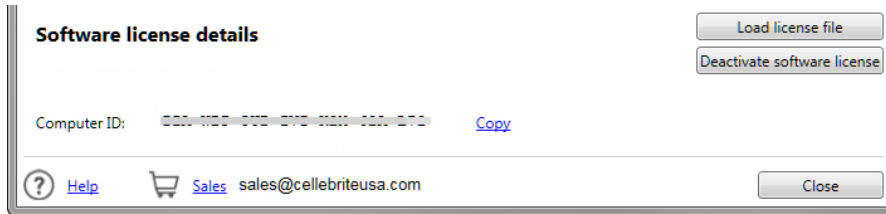
Serial Number

Please select serial number ▼



Activation Code

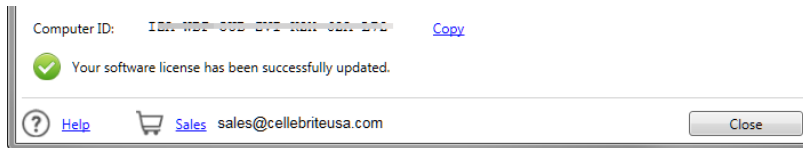
- 8) Next obtain your Computer ID (do not close the MyCellebrite page while performing this step).
- Start the application. The Cellebrite Product Licensing window appears.
  - Click **Copy** to copy the Computer ID displayed in the window.



- 9) In MyCellebrite paste the copied Computer ID.

Computer ID

- 10) Click **Download Now!** to download your application license key to your PC. The license key will also be sent to your registered MyCellebrite email address.
- 11) In the application, click **Load license file** in the Cellebrite Product Licensing window.
- 12) Select the License file and click **Open**. A message appears to indicate that the software license was updated successfully.



- 13) Click Close.

Congratulations, your application is now ready!

#### 2.1.3.4. Using a network dongle

The Network dongle is connected to your organization's network and contains licenses for all the applications purchased.

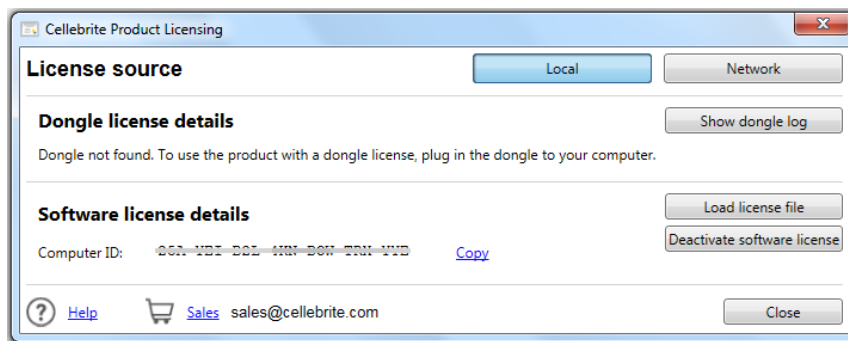


UFED Network Dongles

To use UFED Logical Analyzer with a network dongle:

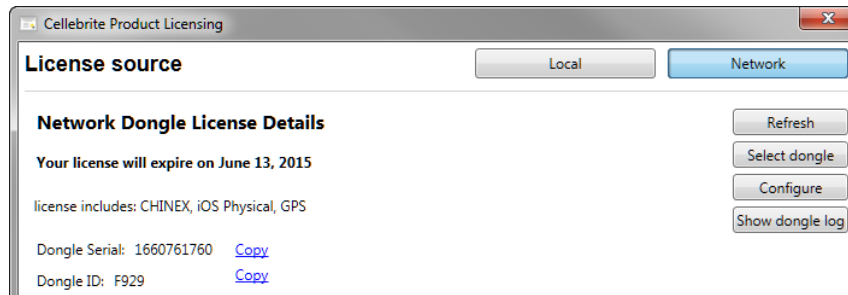
- 14) Start the UFED application. If the network dongle is connected to the network, the application starts and the user can start working immediately.

If the network dongle is not recognized, the Cellebrite Product Licensing window appears.



- 15) Click **Network**. The following window appears.





**NOTE:** If a dongle was not found on the network – make sure that you have an Internet connection and that a dongle is connected to the network. Then click **Refresh** to search for a network dongle again.

**NOTE:** By default the network configuration is set to Broadcast. If required, you can manually connect to the network dongle. Click **Configure** to change the network configuration to Specific host. Enter the host name (or IP address) and the port number (1–5 digits).

**NOTE:** If there is only one network dongle it will be selected automatically. If there are multiple network dongles, select the required dongle from the list and click **Apply**.

**Congratulations, your application is now ready!**

## 2.1.4. Moving UFED Logical Analyzer with a software license to another PC

In cases where a UFED Logical Analyzer installation that has been activated by a software license needs to be moved to another PC, you must first deactivate (remove) the license from the computer.

- 1) In UFED Logical Analyzer, go to **Help > Show License Details**.

The Cellebrite Product Licensing window appears.

- 2) Click **Deactivate software license**.

The Software License Deactivation window appears.

- 3) Click **Copy** to copy the computer ID.

- 4) Go to <http://my.cellebrite.com/deactivation>, and log in to your MyCellebrite account.

If you do not have an account, click **Register now** and create a user. Then return to <http://my.cellebrite.com/deactivation>.

You are directed to the Deactivation wizard.

- 5) Paste the copied computer ID, and click **Next**.
- 6) Click **Download** and download the deactivation file to your computer.
- 7) In UFED Logical Analyzer, go to **Help > Show License Details**.
- 8) Click **Select Deactivation File**, and select the deactivation file that you downloaded in step 6.

Your license is deactivated, and UFED Logical Analyzer creates a deactivation file. The Software License Deactivation window informs you that the deactivation file has been created.

- 9) Return to the Deactivation wizard in <http://my.cellebrite.com/deactivation>.
- 10) Click **Choose File**, and upload the deactivation file created by UFED Logical Analyzer.
- 11) Click **Finish**.
- 12) To get your new UFED Logical Analyzer license, go to <http://my.cellebrite.com/logicalanalyzer>, and follow the license activation steps. For more information, see *Activating UFED Logical Analyzer* (page 19).

### 2.1.5. Enabling connectivity with Windows Vista

Perform the following procedure to enable the UFED unit to connect to PCs running the Windows Vista operating system.

- 1) Go to the Cellebrite Physical Analyzer **Drivers\cbirtucbl** folder.
- 2) Double-click **USB\_Cable\_DRV.exe**.
- 3) Follow the on-screen instructions.



## Chapter 3: Getting started

UFED Logical Analyzer provides powerful presentation and analysis tools for the extracted device data, and simplifies the task of navigating through the device's data types. UFED Logical Analyzer assists you in the complex tasks of intelligence gathering, investigative research, and providing legal evidence in the form of reports.

The application is designed to utilize the UFED unit's logical extraction in a clear and concise way, enabling investigators to use powerful search tools to parse and decode relevant information.

As a completing step, the application enables you to generate reports of your findings and export them in various file formats, such as UFDR, HTML, PDF, Excel (\*.xlsx), and XML.

### 3.1. Start UFED Logical Analyzer

To Start UFED Logical Analyzer, do one of the following:


- Double-click the **UFED Logical Analyzer** desktop shortcut.
- Select **Start > Programs > Cellebrite Mobile Synchronization > UFED Logical Analyzer**.

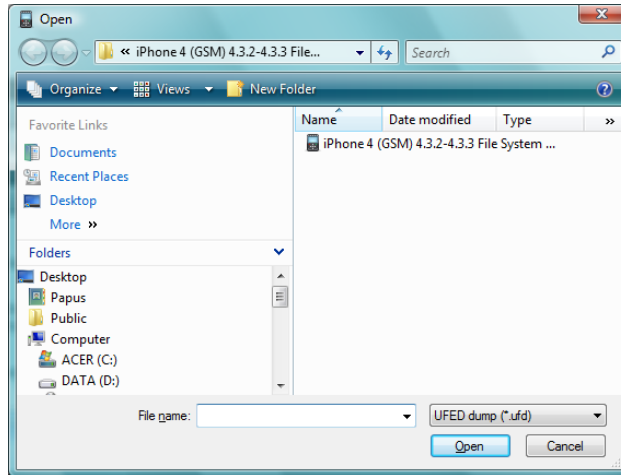
For an overview of the workspace, see *[Orientation to the workspace](#)* (page 43).

## 3.2. Opening a file for analysis

UFED Logical Analyzer can open UFD files created by the UFED device with Logical modules, XML files created by the UFED Physical Analyzer, and UFDR files.

1) Do one of the following:

- In the **Welcome** tab, click **Open**.
- Drag-and-drop the UFD file into UFED Logical Analyzer.
- From the application toolbar, click .
- From the application menu, select **File > Open**.



2) Do one of the following:

- Browse to the location of the file, select it, and click **Open**.
- Drag and drop the file on UFED Logical Analyzer.

The data analysis process begins and runs for several seconds. At the end of the process, a new project is added to the **Project Tree**, and the **Extraction summary** appears in the data display area.

### 3.3. Extracting data to PC

1) Do one of the following:


- Connect the UFED unit to your PC using a USB to mini-USB cable, utilizing the port marked "PC" located on the top of your UFED unit. Your PC may prompt you to install drivers (refer to the UFED Touch User Manual).
- Connect your UFED unit to your PC using the UFED to PC cable (U-441) provided in the UFED Standard and ruggedized kits. Your PC may prompt you to install drivers (refer to the UFED Touch User Manual).



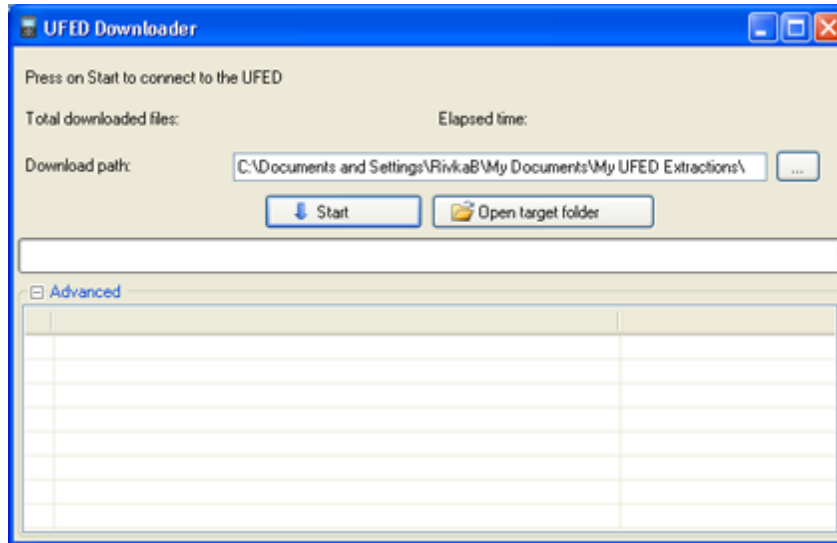
Figure 1: UFED to PC cable


- 2) Connect the source device, using the appropriate cable, to the left USB port of the UFED device.
- 3) On the UFED unit:



- a) From the **Main Menu**, do one of the following:
  - For a logical extraction, select **Logical Extraction**.
  - For a file system extraction, select **File System Extraction**.
- b) Select the manufacturer of the device from the **Select Model** menu.
- c) Select the model of the device.
- 4) On the PC, click **Start > UFED Logical Analyzer** to open UFED Logical Analyzer.  
The **UFED Logical Analyzer** application opens.
- 5) Click the **Read Data from UFED** icon  in the application toolbar.

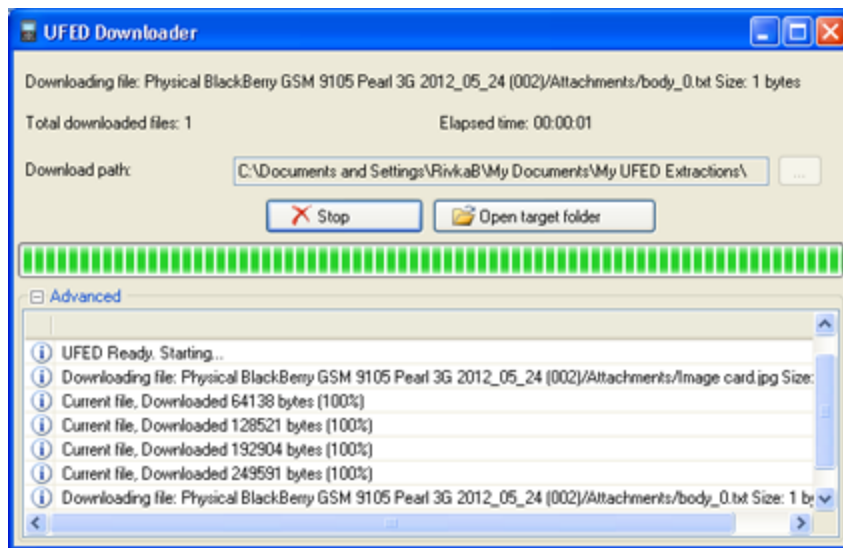
The UFED Downloader window appears.



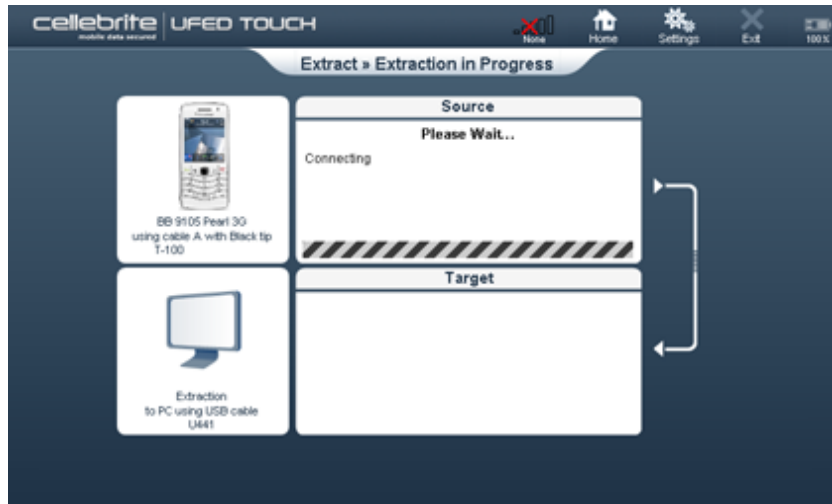
- 6) In the **Download path** area, click  and browse to the desired location for the extraction.  
**Tip:** Click **Open Target Folder** to display the content of the selected target folder.
- 7) On the UFED Touch unit, in the Select Extract Location screen, select **PC**.

- 8) Follow the prompts in the UFED Touch unit until prompted to start the download procedure.
- 9) On the PC, in UFED Logical Analyzer, click **Start** in the UFED Downloader window.

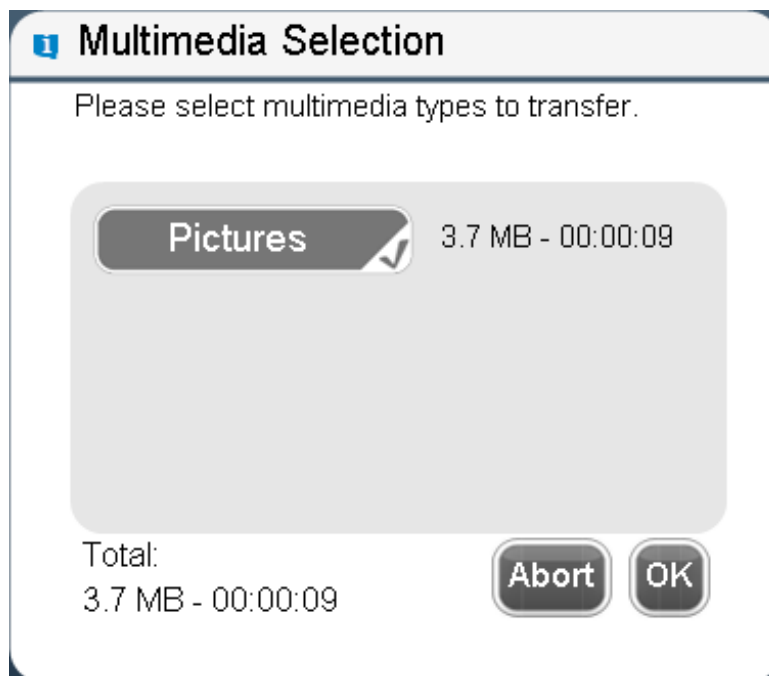
The data transfer from the device to the PC starts.



During the extraction process, the Extraction in Progress screen appears on the UFED unit:



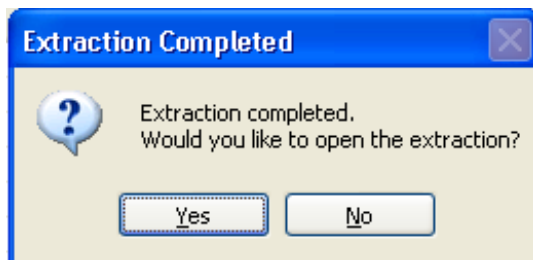
On the UFED unit, you are prompted to select the types of multimedia to include in the extraction:



- 10) Make sure that the media types that you want to include in the extraction are marked with ✓. To cancel the extraction of a particular multimedia type, click ✓ on the multimedia name.
- 11) Click **OK**.

The extraction process continues. When complete, the **Phone Extraction Summary** window appears on the UFED Touch unit.

On the PC in UFED Logical Analyzer, the following message appears:



- 12) Click **Yes**.

The extraction opens in UFED Logical Analyzer and the Extraction Summary screen is displayed.

### 3.4. Saving a project session

Save the project session to save your work on the project, enabling you to close UFED Logical Analyzer and restart your session at a later time.

The saved session file (.pas) includes:

- User selection in the **Analyzed Data** and **Data Files** tables
- Entity bookmarks
- Watch list results
- Opened tabs
- Generated reports
- Unified time zone settings
- Case Information settings

A project session can also be created for extractions performed by third party tools.

**NOTE:** Saved project sessions do not contain defined settings. For more information on how to save your settings, see *[Saving settings](#)* (page 169).

To save a project session:

- 1) In the **File** menu, select **Save Project Session**.

The Save As dialog box appears.

- 2) Browse to the location where you want to save the project session file.
- 3) To change the file name, edit the automatically assigned name in the **File name** box.

**NOTE:** To overwrite an earlier session, choose the same file name.

- 4) Click **Save**.

### 3.5. Loading a project session

- 1) From the **Welcome** tab, open the project that you want to work in.
- 2) In the **File** menu, select **Load Project Session**.
- 3) In the Open dialog box, browse to and select the project session file that you want to open.
- 4) Click **Open**.

The session opens.



### **3.6. Closing a project**

- Do one of the following:
  - In the **File** menu, select **Close**.
  - Right-click the project name and select **Close**.

### **3.7. Closing UFED Logical Analyzer**

- In the **File** menu, select **Exit**.

### 3.8. Keyboard shortcuts

Ctrl+O	Open a file
Ctrl+W	Close a project
Ctrl+P	Open project settings
Ctrl+I	Open iOS wizard
Ctrl+T	Open settings
Space	Select or clear check boxes
Ctrl+R	Open the report wizard
Ctrl+Tab	Switch between open tabs
Ctrl+Home	Move the cursor to the beginning of a table
Ctrl+End	Moves the cursor to the end of a table
Ctrl+B	Add an entity bookmark
Ctrl+U	Open the UFED Downloader to connect to UFED

## Chapter 4: Orientation to the workspace

The workspace contains two main areas; the project tree and the data display area to streamline your workflow.



The workspace contains the following components:

- 1) Application menu bar

- 2) Application toolbar
- 3) Project tree
- 4) Data display area
- 5) All projects search

## 4.1. Project tree

The **Project Tree** area displays the following extracted information structure of each project opened for analysis:

Tree Item	Description
Extraction Summary	<ul style="list-style-type: none"><li>Double-click <b>Extraction Summary</b> to open a summary of the project in the data display area.</li></ul> <p>For more information, see <a href="#">Extraction summary tab</a> (page 57).</p>

Tree item	Description
Device Info	<ul style="list-style-type: none"><li>• Double-click <b>Device Info</b> to open a tab in the data display area.</li></ul> <p>The <b>Device Info</b> tab provides a list of existing information, as well as important identifiers for the device, such as SIM card and user lock codes, where supported. The number of categories and amount of displayed information depends on the device model and manufacturer.</p>

Tree item	Description
Analyzed data	<p>The <b>Analyzed Data</b> tree item displays groups of analyzed data that are related to device-specific features such as contacts, SMS messages, call logs, and so on. The available information and what is displayed depends on the device features, content, and application version. For example, SMS messages are categorized according to the folders used by the messaging feature of the device, such as Drafts, Inbox, Outbox, Sent, and so on. Email messages are categorized according to the account through which they were sent or received. An uncategorized folder contains messages that cannot be categorized in any of the found accounts or account folders (Inbox, Outbox, Drafts, and so on).</p> <p>The following information types may be displayed in <b>Analyzed Data</b>:</p> <ul style="list-style-type: none"><li>• Personal information - Calendar, contacts, notes, call log, user dictionaries, user accounts</li><li>• Messaging items - SMS, MMS, email, instant messages, chat</li></ul> <p>The number in parenthesis designates the number of items each category contains.</p>

Tree item	Description
Data files	<p data-bbox="683 277 1434 378">The <b>Data files</b> tree item sorts the extracted data into common or known file formats, used by devices and computers, such as images, videos, audio, or text files.</p> <p data-bbox="683 400 1434 468">In the Project Tree, the information is displayed in the following categories:</p> <ul data-bbox="683 490 1434 936" style="list-style-type: none"><li data-bbox="683 490 1434 524">• <b>Images</b> - Files that were recognized as image file formats</li><li data-bbox="683 540 1434 574">• <b>Videos</b> - Files that were recognized as video file formats</li><li data-bbox="683 591 1434 624">• <b>Audio</b> - Files that were recognized as audio file formats</li><li data-bbox="683 641 1434 675">• <b>Text</b> - Files that were recognized as text file formats</li><li data-bbox="683 692 1434 759">• <b>Databases</b> - Data structures that were recognized as databases.</li><li data-bbox="683 776 1434 843">• <b>Applications</b> - Files that were recognized as application files (such as .apk, .jar, .dex, .so, .exe files etc.)</li><li data-bbox="683 860 1434 936">• <b>Documents</b> - Files that were recognized as document file formats (such as .doc, .docx, pdf, xlsx, ppt files etc.)</li></ul>

Tree Item	<p><b>Description</b></p> <p>You can create additional data file groups. For more information, see <i>Managing data files settings</i> (page 154).</p>
Tags	<p>Certain file types are identified and tagged in the extracted data.</p> <p>There are eight default tags: <b>Applications</b>, <b>Audio</b>, <b>Configurations</b>, <b>Databases</b>, <b>Documents</b>, <b>Images</b>, <b>Text</b>, and <b>Videos</b>.</p>
Timeline	<ul style="list-style-type: none"><li>• Double-click <b>Timeline</b> to open the device events organized by time in the data display area.</li></ul> <p>The <b>Timeline</b> tab displays the device's time stamped events, such as calls, SMS, MMS, and so on, in a sequential view.</p>



Tree item	Description
Watch lists	<p data-bbox="683 277 1426 378">Watch lists are lists of keywords that you create and then use to search and identify events and items of interest in the extracted data.</p> <ul data-bbox="683 400 1362 461" style="list-style-type: none"><li>• Expand <b>Watch lists</b> to see a list of watch lists that have been run in the current session.</li></ul> <p data-bbox="683 490 1426 523">For more information, see <i>Working with watch lists</i> (page 79).</p>

## Tree Item

## Description

### Entity bookmarks

The entity bookmarks you create are managed in the **Entity Bookmarks** section of the project tree. The number of entity bookmarks in the project is shown in brackets next to the section name.

- Double-click **Entity Bookmarks** to list the entity bookmarks in a tab in the data display area.
- Double-click any entity bookmark to go to the bookmarked item in the appropriate display tab.



For example, double-click an entity bookmark to an SMS message to open the list of SMS messages in an Analyzed Data display tab, with the bookmarked item highlighted.

For more information, see *Bookmarking information (entity bookmarks)* (page 90).

Tree item	Description
Reports	<p>To open a report that has already been generated for the project:</p> <ul style="list-style-type: none"><li>• Double-click the report in the <b>Reports</b> tree item. The report opens in the application associated with the report format.</li><li>• If no reports have been generated for the project, double-click the <b>Reports</b> tree item to open the Generate Report dialog box. For more information on generating a report, see <a href="#">Generating a report</a>.</li></ul>
Project Analytics	<p>The <b>Project Analytics</b> tree item provides you with a comparative analysis overview. You can open an Activity Analytics tab showing an overview of all device activity, as well as tabs that each focus on the phone, email, WhatsApp, Skype, Gmail, and BlackBerry Messenger activities. For more information, see <a href="#">Setting project settings</a> (page 169).</p>

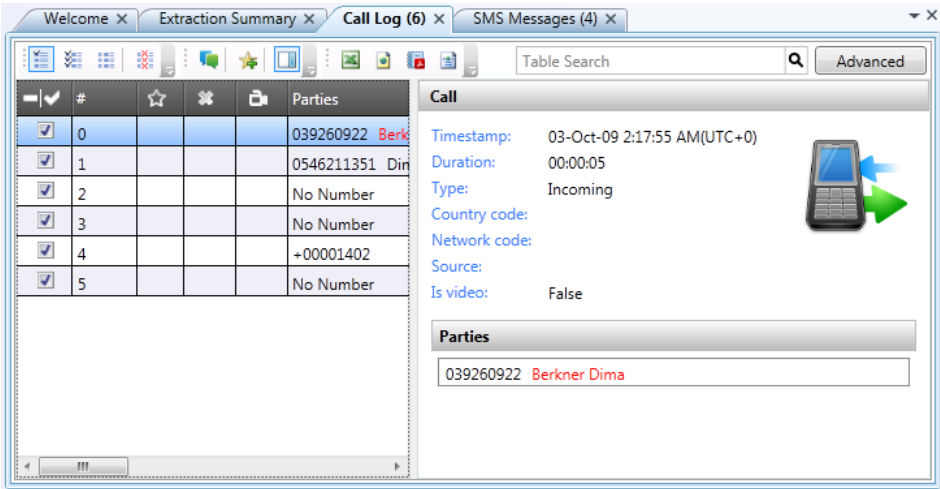
### 4.1.1. Working in the project tree area

Open the tree items to drill down and locate specific information:

- Click to expand or to collapse tree items.
- Double-click a tree item to open detailed information in the data display area.
- Click  at the top of the project tree to expand all the items in the tree.
- Click  at the top of the project tree to collapse all the items in the tree.

## 4.2. Data display area

Double-click an item to display it in a tab. A new tab is opened for each item.



There are four tab types:

- **Welcome** tab
- **Extraction Summary** tab
- Data tabs, with sub-tabs that present a particular view, depending on the data
- **Timeline** tab

The data display area also displays additional windows such as the Trace window, Timeline view, and Watch list results.

#### **To close a tab**

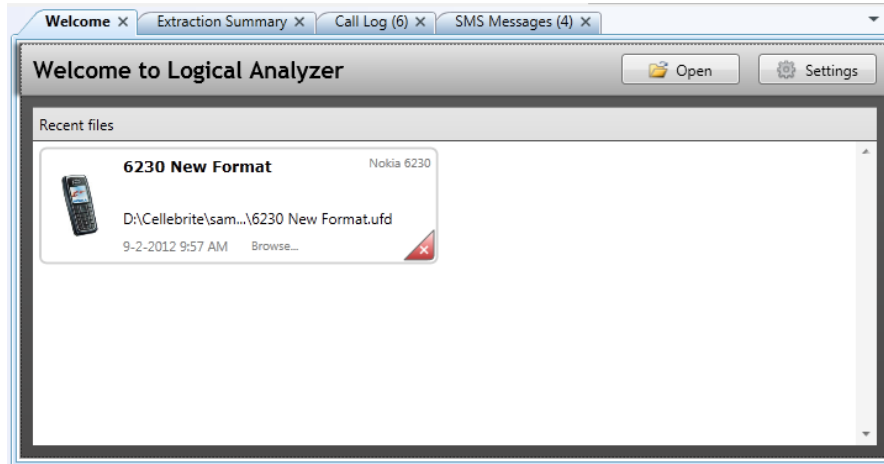
- Do one of the following:
  - Click **X** on the tab header.
  - Click **X** at the top right of the data display area.

#### **To jump to a specific tab**

- At the top right of the data display area, click **▼**, and select the desired tab from the open tabs list.

### 4.2.1. Welcome tab

The **Welcome** tab is automatically displayed in the data display area when the application is launched and displays a list of recently opened files.



Each file in the list is displayed as a framed information group that contains the following items:

- Device picture - A thumbnail image of the device from the application resources, if available. When unavailable, a general placeholder image is used.
- File name - The name of the opened file, without the file extension.

- File path - The file system path to the file location.
- Device model - The identified device manufacturer and model, or BINARY if the opened file was a binary extraction.
- Case name - If the report was given a case name, the name is shown. The name can be defined in the project settings.
- Date and time - The date and time stamp in which the file was last opened.
- Browse link - A direct link to the file in the system.
- Remove recent item - Click to remove the item from the **Welcome** tab.

You can do the following:

- Click on a framed item to open the files for decoding.
- Click **Browse** to go directly to the file associated with it in the file system.
- Close the **Welcome** tab. To reopen it, go to **View > Show Welcome**.



### 4.2.2. Extraction summary tab

The **Extraction Summary** tab is displayed automatically whenever you open a new extraction for analysis.



- To reopen the tab if closed, double-click the **Extraction Summary** tree item.

The **Extraction summary** tab can display the following information:

- **Extraction Info** - Information related to the device extraction. Such as:

<i>Extraction start date/time</i> <i>Extraction end date/time</i>	When the extraction started and ended.
<i>Unit Identifier</i>	The serial number of the device that performed the extraction (e.g., UFED Touch), or a unique ID if the extraction was performed by a PC application (e.g., UFED 4PC).
<i>Unit Version</i>	UFED software version (e.g., 4.1.0.220)
<i>Selected Manufacturer</i>	Manufacturer of the device (e.g., Apple)
<i>Selected Device Name</i>	Device name (e.g., iPhone 4)
<i>Connection Type</i>	Cable used for the extraction (e.g., Cable No. 100)
<i>Extraction Type</i>	Type of extraction performed (e.g., Logical)
<i>Extraction ID</i>	Unique ID for each extraction type

- **Device Info** - A summary of the specific device info pulled from the extraction file. See the *Device Info* item in [Project tree](#) (page 44).
- **Device Content** - Analyzed content, divided into the following categories:

- **Phone Data** - The types of analyzed device data found in the extraction, such as call log, contacts, SMS messages, and so on. For the complete list of phone data types, see the *Analyzed Data* item in *Project tree* (page 44).
- **Data Files** - The types of standard data files found in the extraction, such as images, videos, audio, and text files. See *Data files* (page 151).

To display the relevant information in a new tab in the data display area:

- Click any of the tree items.

### 4.2.3. Data tabs

Data tabs show files of a specific type (such as call log, contacts, SMS messages, and so on).

Each type of data file has several data display modes:

Image files	Image View and File Info
Video files	File Info
Audio files	File Info
Text files	File Info

Databases

Database View and File Info

Document files

File Info

Data tabs display the data in a variety of sub-tabs, depending on the data type:

- **Text view** - View text files as text.
- **Table view** - A list of all the files of a specific type (images, videos, audio, text, and so on) that were found during the data analysis process.
- **Folder view** - View the folder structure of the data files paths in the reconstructed file system (for data files only).
- **Image view** - View the image. See [Viewing image files](#) (page 67).
- **Thumbnail view** - View images by thumbnail (for images only).
- **File Info** - View information about the file.

#### 4.2.3.1. Working in data tabs

##### Selecting Items

Select items in the data display area to include them in any report you generate. By default, all items are selected.

- To select multiple items, hold the SHIFT or CTRL keys (consecutive and nonconsecutive selection).
- When an item is selected, press the space bar to select or clear the check box, which indicates if the item should be included or excluded from the report.
- To select all items at once, check the box in the column header (table view and timeline) or check the **Select all** check box (thumbnail view).

### Sorting columns

Sort each column alphabetically or by time.

- Click the column header to toggle the order.

### Re-ordering the columns

For your convenience, you can change the order of the columns. Your preference is retained for the duration of the session.

- Drag the desired column to the desired location.

### Hide or show columns







- Right-click the column header and select the column name in the list.

### Viewing more information

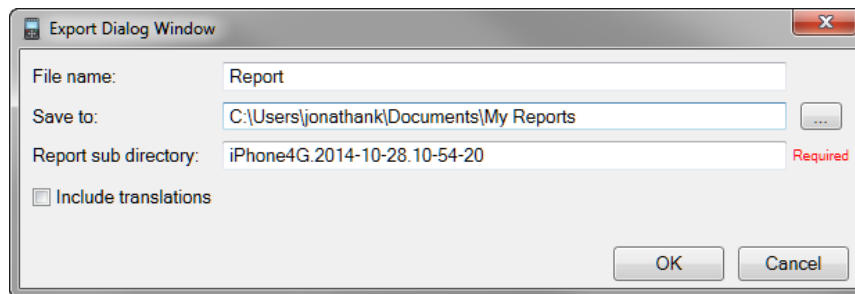
For data tabs containing textual information, by default the right pane is open, displaying the selected item's information.


- To close or open the right pane, click .

## Exporting data

- 1) To export the data in a particular tab, click the desired output in the toolbar: Excel , HTML , PDF , XML , KML  (location data only), or EML  (email data only).

The Export Dialog Window appears.



- 2) Do one of the following:
  - Enter the path where you want to save the report
  - Click  and browse to and select the desired location.
- 3) Select the **Include translations** check box to include translated data.
- 4) Click **OK**.

The report is generated, and a message appears asking if you would like to open it in third party software.

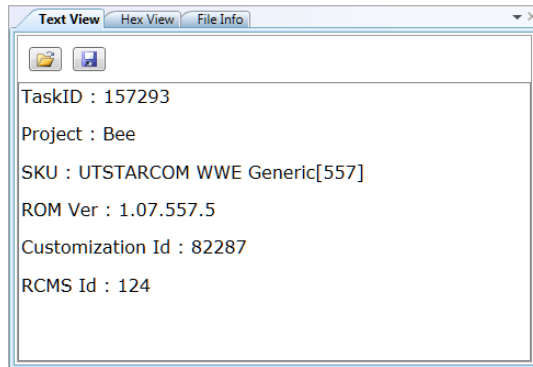
- 5) Click **Yes** or **No**.

The file is opened in the default third party software.

**NOTE:** When exporting to EML, a file is created for each email.

#### 4.2.3.2. Text view

For text-based data files, view the data as text.



### 4.2.3.3. Table view for data files

For data files, the table shows the following information:



Indicates whether to include (checked) or exclude (unchecked) the item in the report generated.

#

Row number.



Indicates if the item is bookmarked.



Indicates whether the data file was deleted , or has an unknown status ("?" or white document icon).

Image

A thumbnail of the image or an icon of the file type. (Image data files only).

Name

The file name.

Path

The root path of the data file.

Size

The size of file.



<b>Metadata</b>	Additional metadata of the data file.
<b>Created</b>	The creation time stamp of the data file.
<b>Modified</b>	The modification time stamp of the data file.
<b>Accessed</b>	The last access time stamp of the data file.
<b>Bookmark Note</b>	Details of the bookmark.

In addition, indicators are displayed to show attachments, indicate video calls, and to show even direction.

#### 4.2.3.4. Table view for analyzed data

For analyzed data, table view tabs display a list of all the events of a specific type (Call Log, Contacts, SMS messages, and so on) that were found during the data analysis process.

The screenshot displays the Cellebrite software interface. At the top, there are tabs for 'Welcome', 'Extraction Summary', 'Extraction Summary', 'Images', and 'Call Log (12)'. The 'Call Log (12)' tab is active. Below the tabs, there is a 'Table View' section with a table of call events. The table has columns for a checkbox, a number, a star icon, a trash icon, and a 'Parties' column. The table contains 12 rows of data. To the right of the table, there is a 'Call' details panel. It includes a 'Table Search' bar with a magnifying glass icon and an 'Advanced' button. Below the search bar, the 'Call' details are displayed: 'Timestamp: 07-Jan-04 9:42:00 PM', 'Duration:', 'Type: Outgoing', 'Country code:', 'Network code:', 'Source:', and 'Is video: False'. There is also an icon of a mobile phone with a green arrow pointing to it. Below the 'Call' details, there is a 'Parties' section with a text box containing the number '0526765424'.

<input checked="" type="checkbox"/>	#	☆	🗑️	Parties
<input checked="" type="checkbox"/>	1			0526765424
<input checked="" type="checkbox"/>	2			0547265478
<input checked="" type="checkbox"/>	3			032535522 Pet store
<input checked="" type="checkbox"/>	4			0546512487
<input checked="" type="checkbox"/>	5			0543774742
<input checked="" type="checkbox"/>	6			038582555 Slater Paul
<input checked="" type="checkbox"/>	7			0576761249
<input checked="" type="checkbox"/>	8			0527623485
<input checked="" type="checkbox"/>	9			0546608889
<input checked="" type="checkbox"/>	10			0508159490
<input checked="" type="checkbox"/>	11			*111
<input checked="" type="checkbox"/>	12		🗑️	0526765424

**Call**

Timestamp: 07-Jan-04 9:42:00 PM  
Duration:  
Type: Outgoing  
Country code:  
Network code:  
Source:  
Is video: False

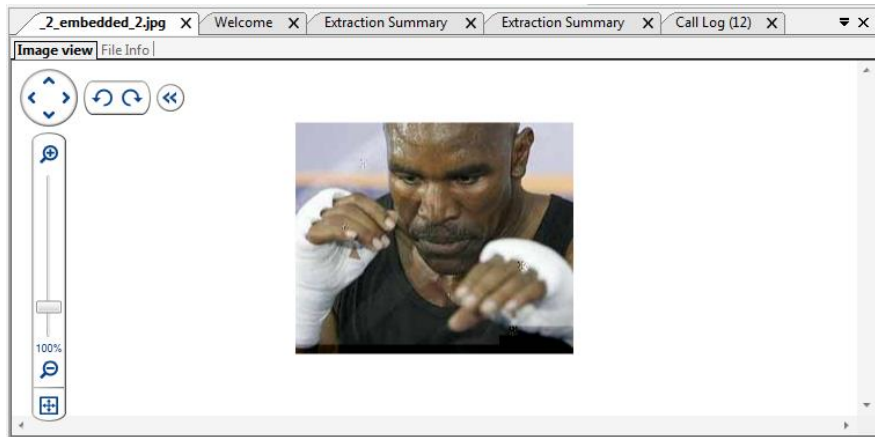
**Parties**

0526765424

### 4.3. Viewing image files

- 1) Double-click an image in a data display tab.

A new tab opens containing the image. The tab is divided into two sub-tabs; **Image view** and **File Info**.



- 2) In the **Image view** tab, use the image controls:



When the image is enlarged, navigate the image.



Rotate image clockwise and anti-clockwise.



Zoom in and out. You can also adjust the zoom using the slider.



Zoom to fit the tab.



Reset the zoom to 100%.



Hide image controls.

- 3) Click the **File Info** tab to view the file information. For example, the File metadata section includes information such as the Capture Time, which is the date and time a photo was taken.

## 4.4. Playing video files

To play the video within UFED Logical Analyzer:

- 1) In the data table, double-click the media file that you want to play.

A new tab opens for the media file.

- 2) Click .

To play the video in the default program:

- Right-click the media file and select **Open with default program**.

## Chapter 5: Locating and analyzing information

This section describes how to browse, search, filter, bookmark, and manage the information in your project.

### 5.1. Searching for information in a data tab

In **Table View** tabs, search for a particular item within the data table. The search is performed on all the data entries within the table.

- In the **Table Search** box, enter any string.

The table updates to display only items containing the string you entered.

### 5.2. Using the quick filter

Use the quick filter tools to filter data in **Table View** tabs as follows:



Show all

Displays all items



Only selected

Displays items that are selected



Only not selected

Displays items that are not selected



Deleted

Displays deleted items



Show all

Show all images



Display images above 30KB

Display only small images above 30KB.



Display images above 100KB

Display only medium-sized images above 100KB.



Display images above 500KB

Display only large images (500+KB)



Filter images (by extension)

Click to enable file type filtering:



Show JPEG

Display JPG or JPEG files



Show GIF

Display GIF files



Show BMP

Display BMP files



Show PNG

Display PNG files



Metadata filter

Filter image and video files by Metadata (All, Without metadata or Has metadata) and Location (All, Has location or Without location).



Capture filter time

Filter image and video files by capture time. The maximum range is displayed by default, and you can select a specific date and time range.



Translation filter

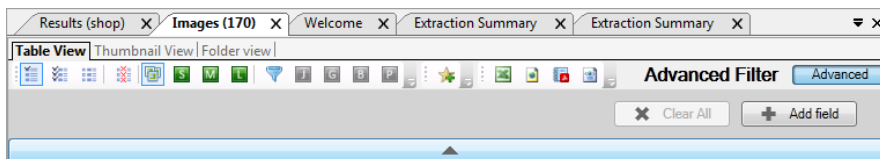
Filter translated text to display all text, translated text or text that has not been translated.

**NOTE:** The toolbar items are context-sensitive, and only appear when relevant data is displayed.

## 5.3. Using the advanced filter

Use the advanced filter to filter the list based on a combination of several parameters.

- 1) In the filter toolbar, click **Advanced**.




- 2) Click **Add field**, and select a field from the drop-down list. The fields list comprises the columns in the current data tab.
- 3) In the box that appears for the selected field, enter any string or timestamp.


The tab displays only items that match the filter.

- 4) To add additional filters, repeat steps 2-3.

When you place additional filters in the Advanced search, the returned results match all specified criteria.

- 5) To clear the string you entered, click .
- 6) To clear all the entered strings, click **Clear All**.



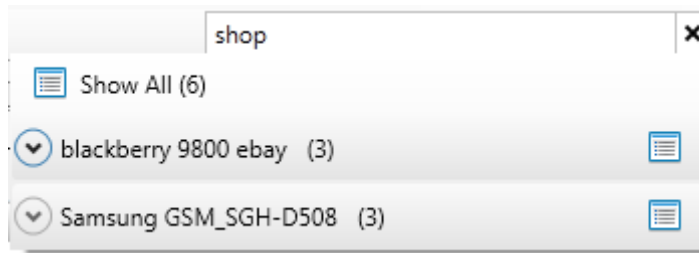
- 7) To remove the field filter, click .
- 8) To close the advanced filter, click **Advanced**.

## 5.4. Searching for information in all open projects

Use the **All projects** search box in the toolbar to search for information in all open projects.


- 1) Type any string in the **All Projects** box.

A list of matching results appear under the **All Projects** search field. The results are sorted by open project. Within each open project, the results are sorted by categories according to type (SMS, messages, contacts, files, and so on). The number of matching results found in each type category is also displayed.



- 2) Click  to collapse or expand the projects.

3) Do one of the following:

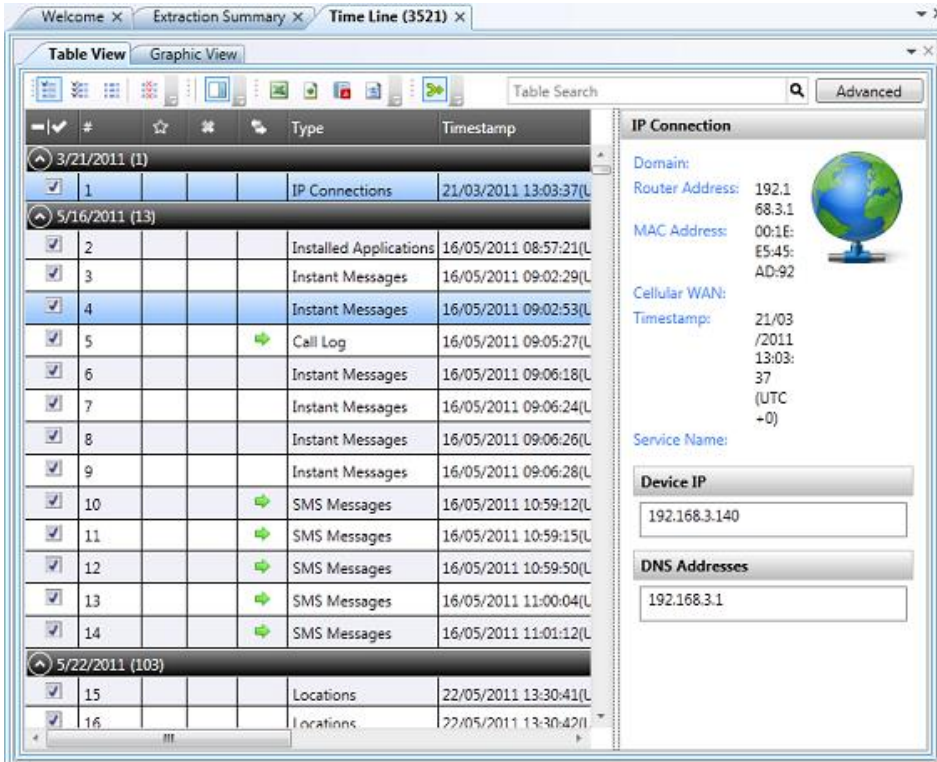
- Click  next to the project name to view the results of the search in that extraction in a tab in the data display area.
- Select **Show All** from the top of the quick results list to display a results tab in the data display area listing all the matching search results. The matching string in each item is colored in red.  
As in the quick results list, the results tab lists the results by type.

## 5.5. Timeline view

Timeline view is a powerful tool that enables you to analyze data in chronological order, to identify the order of events and make connections between them.

Timeline view has two views; table and graphic.

In table view, the events are displayed in a table, organized by date and time.



The screenshot displays a software interface with a 'Table View' tab selected. The table lists events organized by date and time. The right sidebar shows details for the selected event, including IP connection information and device IP.

	#	Type	Timestamp
3/21/2011 (1)			
<input checked="" type="checkbox"/>	1	IP Connections	21/03/2011 13:03:37(L
5/16/2011 (13)			
<input checked="" type="checkbox"/>	2	Installed Applications	16/05/2011 08:57:21(L
<input checked="" type="checkbox"/>	3	Instant Messages	16/05/2011 09:02:29(L
<input checked="" type="checkbox"/>	4	Instant Messages	16/05/2011 09:02:53(L
<input checked="" type="checkbox"/>	5	Cell Log	16/05/2011 09:05:27(L
<input checked="" type="checkbox"/>	6	Instant Messages	16/05/2011 09:06:18(L
<input checked="" type="checkbox"/>	7	Instant Messages	16/05/2011 09:06:24(L
<input checked="" type="checkbox"/>	8	Instant Messages	16/05/2011 09:06:26(L
<input checked="" type="checkbox"/>	9	Instant Messages	16/05/2011 09:06:28(L
<input checked="" type="checkbox"/>	10	SMS Messages	16/05/2011 10:59:12(L
<input checked="" type="checkbox"/>	11	SMS Messages	16/05/2011 10:59:15(L
<input checked="" type="checkbox"/>	12	SMS Messages	16/05/2011 10:59:50(L
<input checked="" type="checkbox"/>	13	SMS Messages	16/05/2011 11:00:04(L
<input checked="" type="checkbox"/>	14	SMS Messages	16/05/2011 11:01:12(L
5/22/2011 (103)			
<input checked="" type="checkbox"/>	15	Locations	22/05/2011 13:30:41(L
<input checked="" type="checkbox"/>	16	Locations	22/05/2011 13:30:42(L

**IP Connection**

Domain:

Router Address: 192.168.3.1

MAC Address: 00:1E:5E:45:AD:92

Cellular WAN:

Timestamp: 21/03/2011 13:03:37 (UTC +0)

Service Name:

**Device IP**

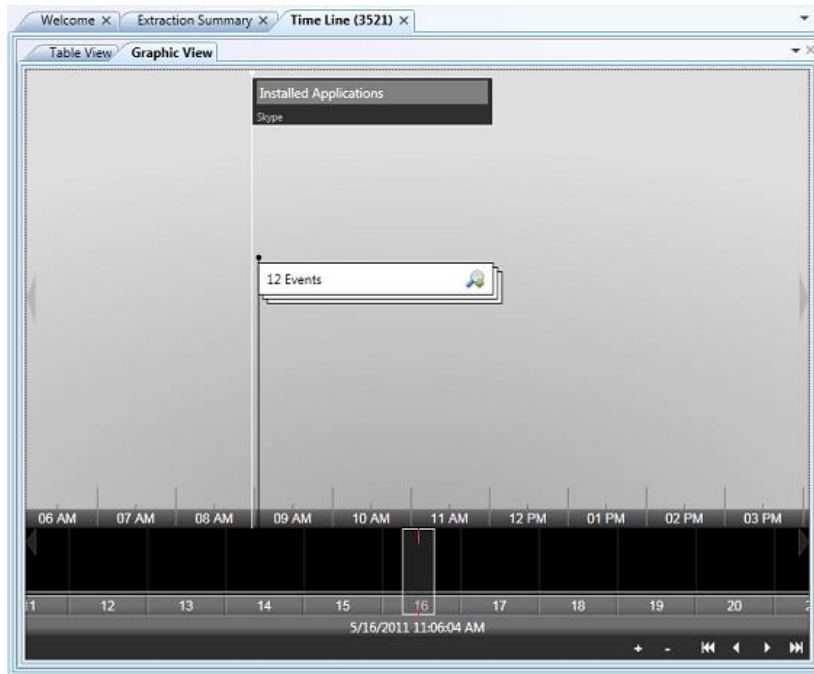
192.168.3.140


**DNS Addresses**

192.168.3.1



- Click  to group or ungroup the events by date.

In graphic view, the events are displayed in a graph, enabling you to quickly identify activity spikes that may be of interest.



- To scroll forwards and backwards in the timeline, use the , ,  and  buttons.

You can increase or decrease the level of detail in the Timeline Graph View:

- To increase the time resolution, click .
- To decrease the time resolution, click .


Events that occur within close proximity are flagged in groups.

- Click  to open another timeline view tab for the group of events.

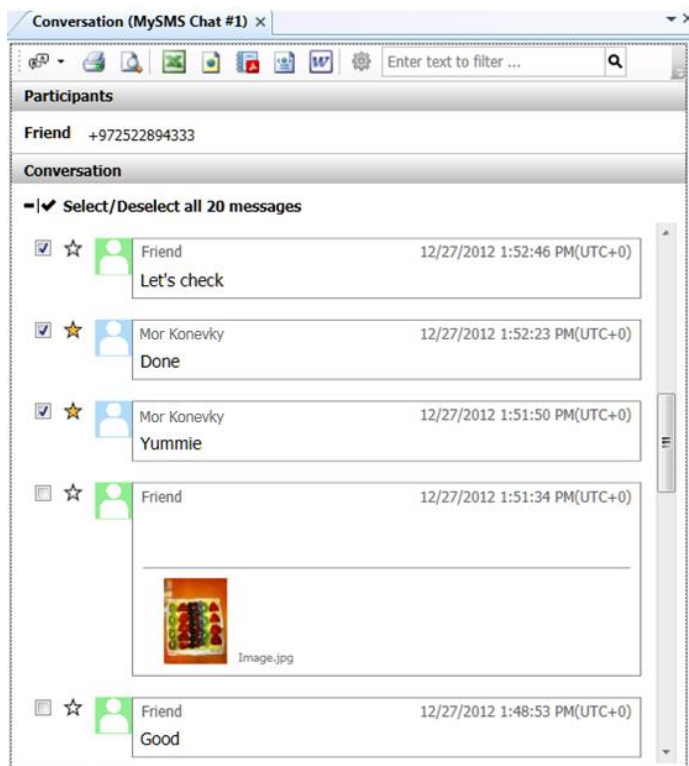
### 5.6. Accessing conversation view











Communication-based data, such as call logs, email, SMS and MMS messages, and so on, can be displayed in a conversation view layout for easier and better tracking over the communication between two or more parties. You can search for messages within a chat, select the messages to include within a report (by default all chat messages are included), print, or export the conversation.

**To access and use conversation view:**

- 1) In a communication-based data table, select one of the records.
- 2) Click .

A conversation tab opens, displaying related items as a conversation between the sending and receiving parties of the selected item.



- 3) To translate or delete translated text, click  and then select **Translate all** or **Delete all translations**.
- 4) To print the conversation, click .
- 5) To view a print preview, click .
- 6) To export the conversation, click the desired output in the conversation tab toolbar:  
Excel , HTML , PDF , XML , or Word .
- 7) To change the order of the conversation, click  and then select **Oldest message first**, or **Newest message first**.
- 8) To filter messages, enter text in the search box.
- 9) To add or edit bookmarks, click .
- 10) Select a check box to include specific messages in the report, (or select all messages or no messages).


## 5.7. Working with watch lists

Run a watch list of keywords against your extracted data to identify and highlight important and relevant information.

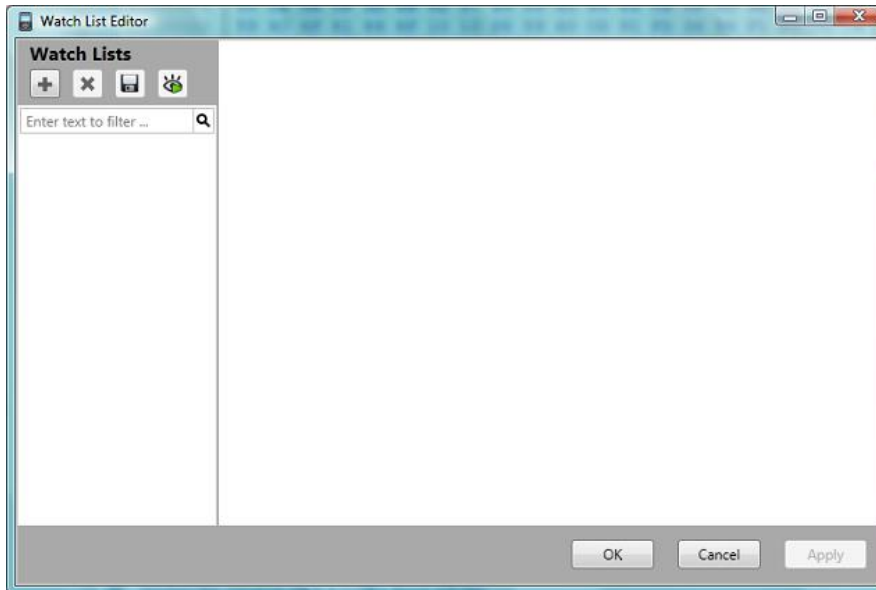
The watch list search can either be activated automatically or run manually on selected decoded data.

### 5.7.1. Creating a watch list

1) Do one of the following:

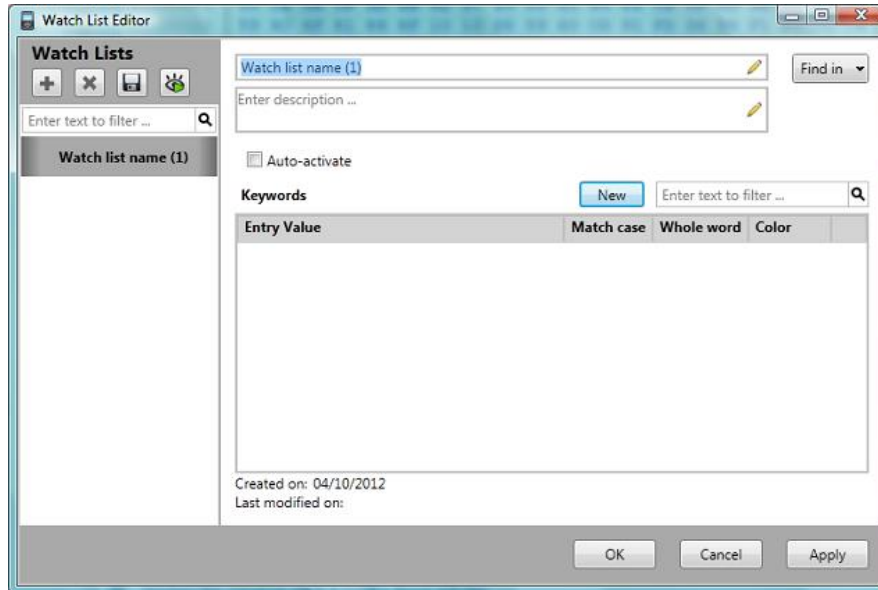
- In the toolbar, click .
- In the **Tools** menu, select **Watch List Editor**.

The Watch List Editor appears.



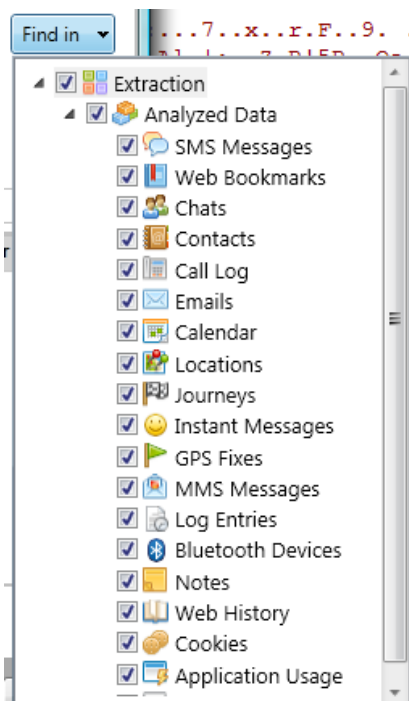


- 2) Click , and select **New**.



- 3) In the **Watch list name** box, enter a name for the watch list.


- 4) To set the watch list to find keywords only in data types in the project, click **Find in**, and select the desired data types.



When you run the watch list, only selected data types are checked for matches.


- 5) In the **Enter description** box, enter a general description for the watch list (optional).
- 6) To set the watch list to run automatically when you open projects, click **Auto-activate**.
- 7) Click **New** to add a new keyword.

A new keyword row appears in the Keywords list.

- 8) For each keyword, set the following, as desired:
  - **Entry Value:** Enter the keyword.
  - **Match case:** Select to match the case of the keyword
  - **Whole word:** Select to match the whole keyword.
  - **Color:** Click  and select the color you want matched keywords to be shown in.
- 9) Do one of the following:
  - Click **Apply** to save the watch list and keep the Watch List Editor open.
  - Click **OK** to save the watch list and close the Watch List Editor.
  - Click **Cancel** to close the Watch List Editor without saving your changes.

### 5.7.2. Editing a watch list

- 1) In the Watch List Editor, select the watch list that you want to edit.
- 2) Edit the watch list parameters and keywords that you want to change.
- 3) To filter the keyword list to locate a particular keyword, type the keyword in the **Enter text to filter** box.

- 4) To edit a keyword, click the relevant keyword in the list, and make the desired changes.
- 5) To delete a keyword, click .
- 6) When you have finished making changes, do one of the following:
  - Click **Apply** to save the watch list and keep the Watch List Editor open.
  - Click **OK** to save the watch list and close the Watch List Editor.
  - Click **Cancel** to close the Watch List Editor without saving your changes.


### 5.7.3. Importing a watch list

The export and import functions enable you to share watch lists and receive watch lists from your colleagues. Import existing watch lists (\*.csv files) that were saved from or created by UFED Logical Analyzer.























You can also import a CSV file that contains a list of keywords, which can then be used as watch list keywords. This option will import the keywords without any formatting and will look to find all data types by default.

- 1) In the main toolbar, click .

The Watch List Editor appears.

- 2) Click , and select **Import**.
- 3) Browse to the location where your watch list is saved, select the CSV file, and click **Open**.

The watch list appears in the Watch List Editor. An example is displayed next.

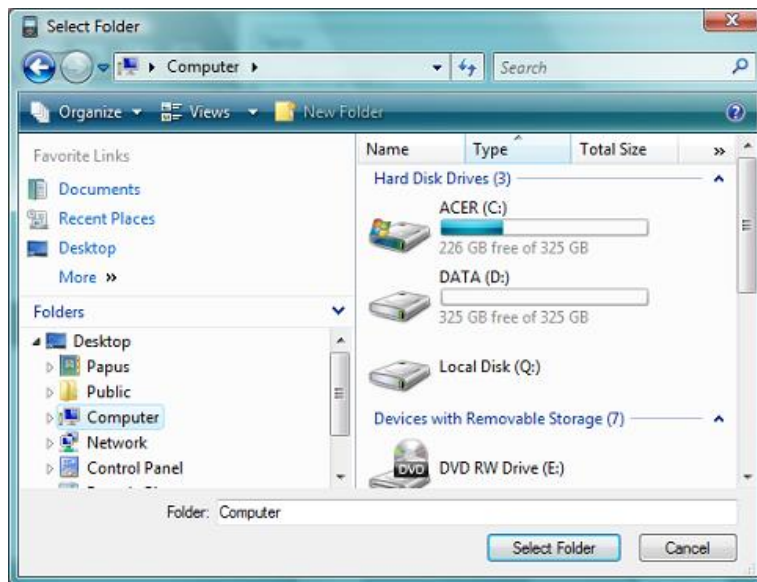
Keywords				
		New	Enter text to filter ...	Q
Entry Value	Match case	Whole word	Color	
ACID HEAD	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
ANGEL DUST	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
BAG	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
BALLOON	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
BRICK	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
BROWNIES	<input type="checkbox"/>	<input type="checkbox"/>		
CANDY	<input type="checkbox"/>	<input type="checkbox"/>		
CANDYMAN	<input type="checkbox"/>	<input type="checkbox"/>		
COKE	<input type="checkbox"/>	<input type="checkbox"/>		
COOKER	<input type="checkbox"/>	<input type="checkbox"/>		
CUT	<input type="checkbox"/>	<input type="checkbox"/>		

5.7.4. Exporting a watch list

Export watch lists to save the watch list as a \*.csv file for later use, or to share with others.

1) In the Watch List Editor, select the watch list that you want to export.

2) Click .



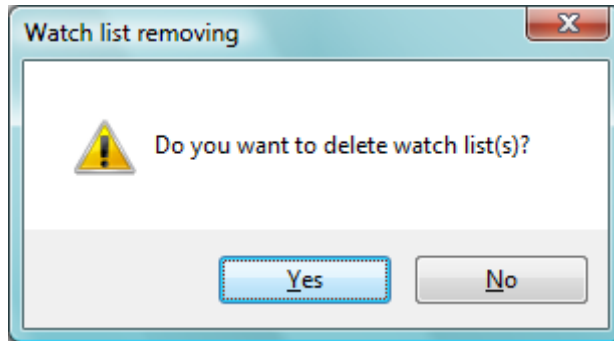
3) Browse to the location where you want to save your watch list, and click **Select Folder**.

4) The watch list is exported. It will be saved by default as [name of watch list].csv.

### 5.7.5. Deleting a watch list

- 1) In the Watch List Editor, select the watch list that you want to delete.

- 2) Click .



- 3) Click **Yes**.

The watch list is deleted.

## 5.7.6. Running a watch list

You can run watch lists on open projects.

### 5.7.6.1. Running a watch list on particular projects

When you run a watch list from the Watch List Editor, you can select which watch lists to run, and on which projects you want to run them.

- 1) In the toolbar, click  to open the Watch List Editor, and select the watch list you want to run.

- 2) Click .

A list of open projects appears.

- 3) Select the open project(s) that you want to run the search on.

**NOTE:** A tick mark  shows that the selected watch list is currently active for the project.

- 4) Click **Apply**.

UFED Logical Analyzer searches for keywords in the selected project(s). When complete, the watch list results appear in the **Watch Lists** tree item.

If the watch list is assigned to only particular information types (see [Creating a watch list](#) (page 80)), only matches to those types appear in the watch list results.



### 5.7.6.2. Running a watch list on your current project

When you run a watch list from the project tree, you can select which watch lists to run on the project that you are currently working in. If you have more than one project open, the selected watch lists run on the project that you last clicked in in the project tree.


- 1) In the toolbar, click .

A list of watch lists appears.

- 2) Select the watch list(s) that you want to run on the project you are currently working in.

**NOTE:** A tick mark  shows that the watch list is currently active for the project.

- 3) Click **Apply** on the project that is in focus in the project tree.

**NOTE:** When you click  from the toolbar, you can only run the watch list(s) on the project that you last clicked in in the project tree.

UFED Logical Analyzer searches for keywords in the selected project(s). When complete, the watch list results appear in the **Watch Lists** tree item.





If the watch list is assigned to only particular information types (see [Creating a watch list](#) (page 80)), only matches to those types appear in the watch list results.

## 5.8. Bookmarking information (entity bookmarks)

An entity bookmark is a quick reference pointer you can create on individual items:


- An **Analyzed Data** item such as a call from the call log, a contact record, an email message, etc. See the *Analyzed Data* item in *Project tree* (page 44).
- A **Data Files** item such as an image file, a video file, a text file, and so on. See the *Data files* item in *Project tree* (page 44).

The entity bookmarks you create are managed in the **Entity Bookmarks** tree item. The number of entity bookmarks in the project is shown in brackets next to the section name.

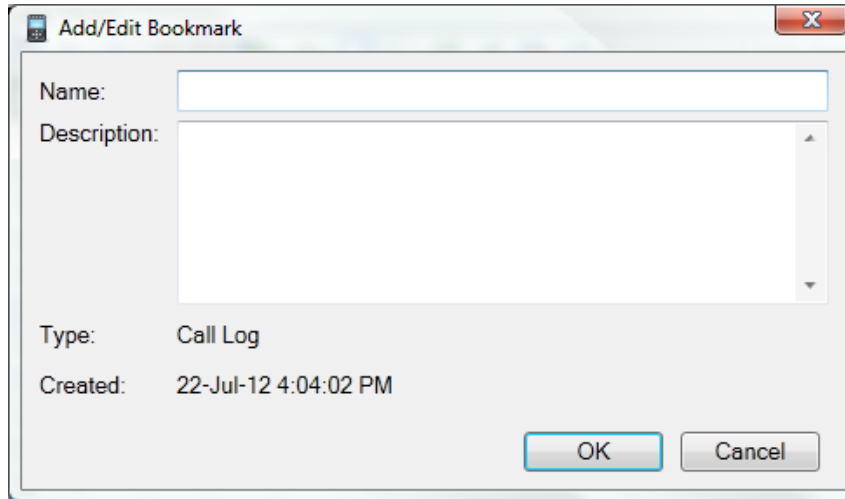
- Double-click **Entity Bookmarks** to list the entity bookmarks in a tab in the data display area. Selected entity bookmarks are included in reports that you generate.
- Double-click any entity bookmark to go to the bookmarked item in the appropriate display tab.  
For example, double-click an entity bookmark to an SMS message to open the list of SMS messages in an Analyzed Data display tab, with the bookmarked item highlighted.
- Hover over a ★ to display the bookmark name and description.
- To print or export just the entity bookmarks list, click the desired output in the **Entity Bookmarks** tab toolbar: Excel , HTML , PDF , or XML .

### 5.8.1. Creating a new entity bookmark

Entity bookmarks can be added to items in Table view.


- 1) Select the item you want to bookmark.
- 2) Click .

The Add/Edit Bookmark dialog box appears.





The image shows a screenshot of the 'Add/Edit Bookmark' dialog box. The dialog has a title bar with a close button (X). Inside, there are two input fields: 'Name:' with a text box and 'Description:' with a larger text area. Below these, the 'Type:' is set to 'Call Log' and the 'Created:' timestamp is '22-Jul-12 4:04:02 PM'. At the bottom right, there are 'OK' and 'Cancel' buttons.

- 3) Enter a name and a description to the new entity bookmark, then click **OK**.

A new entity bookmark pointing to the selected item is added to the entity bookmarks list of the project. The bookmarked item record is marked with a .



### 5.8.2. Editing an entity bookmark

- 1) Select one of the following:
  - An entity bookmark record from the list of **Entity Bookmarks** in the project tree.
  - A bookmarked item (marked with .
- 2) Click  in the Table view toolbar.

The Add/Edit Bookmark dialog box appears.

- 3) Edit the name or description, then click **OK**.

### 5.8.3. Deleting an entity bookmark

- 1) Select one of the following:
  - An entity bookmark record from the list of **Entity Bookmarks** in the project tree.
  - A bookmarked item (marked with .
- 2) Click  in the Table view toolbar.

The bookmark is deleted.

# Chapter 6: Translating decoded data

Translate the content in your extractions that are in foreign languages without having to wait for a translator to become available, or to use Internet-based tools.

The Translation feature enables you to translate decoded data on demand, so that an investigator can understand the information available in an extraction. The Translation feature is an offline translation solution, where you do not need to be connected to the Internet. You can select single, multiple or all table entries for translation. Both the original and the translated text can be included in the report.

The lists of supported languages are as follows:

Chinese (Simplified)	Japanese (requires additional payment)
Chinese (Traditional)	Korean
Dutch	Polish
German	Portuguese
Hebrew	Russian
Italian	Spanish
French	Ukrainian

## 6.1. Using the feature

To use this feature, you need do the following:

- Update your license with the selected translation languages
- Download the translation pack
- Translate the decoded data

## 6.2. Updating your license with the selected languages

You can select up to five languages for free from the My Products page in [MyCellebrite](#). If additional languages are required, you can purchase the Basic Language Package. You cannot change a language after saving, but you can request [additional languages](#).

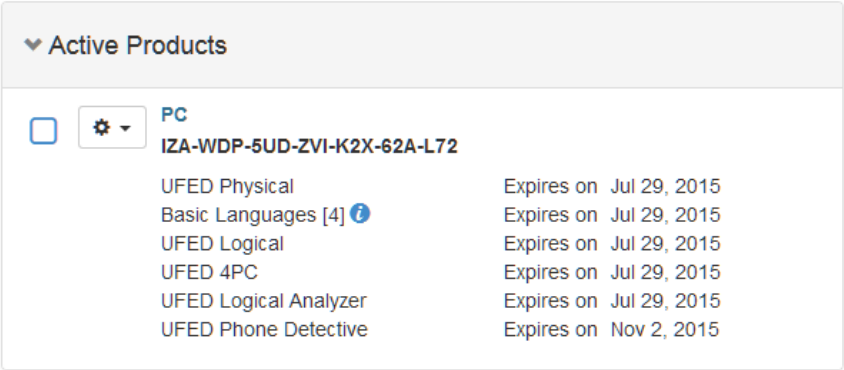
**NOTE:** If you want to translate to a language other than English, you should select it as well.

After updating your product license with the selected languages, you can use the following procedure to review the languages included in the translation license.

### 6.2.1. Selecting languages in MyCellebrite

To select languages:

1) Log in to MyCellebrite and select the **My Products** tab. The following window appears.



2) Select  and click **Select Languages**. The following window appears.

Device Languages for IZAWDP5UDZVIK2X62AL72

Choose up to 5 languages for translating decoded data.  
Tip: If you want to translate to a language other than English you should select it as well.  
You cannot change a language after saving, but you don't have to choose all 5 right now.

Select Language ▲

Select Language ▲

Select Language ▲

Select Language ▲

Select Language ▲

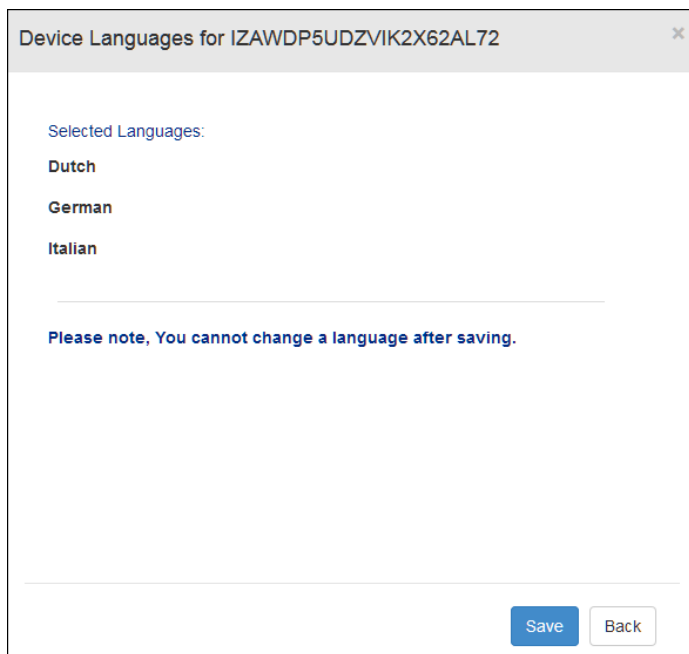
Need more languages?

Next

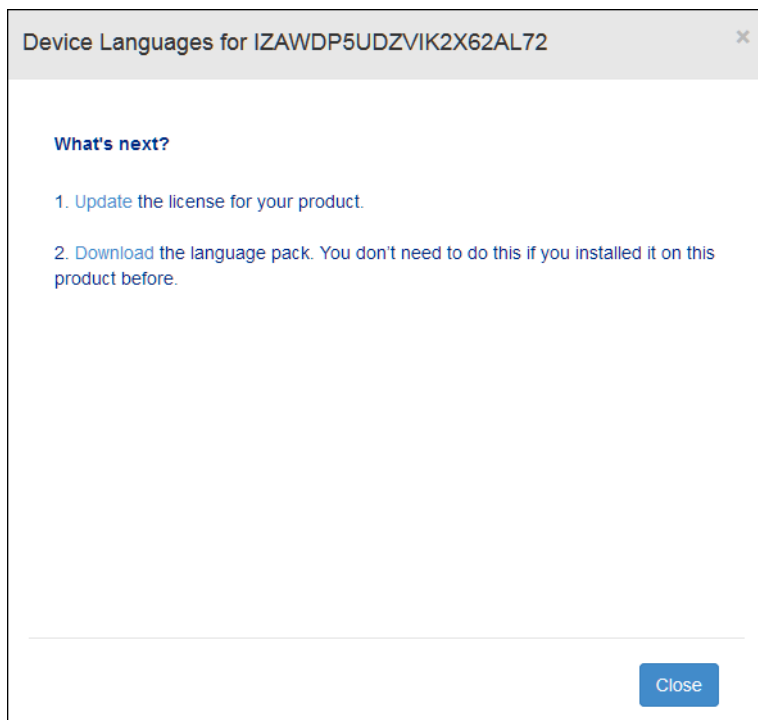
Cancel

- 3) Select up to five translation languages and click **Next**. The following window appears. For additional languages, click **Need more languages** and complete the form.





- 4) Click **Save**. The following window appears.



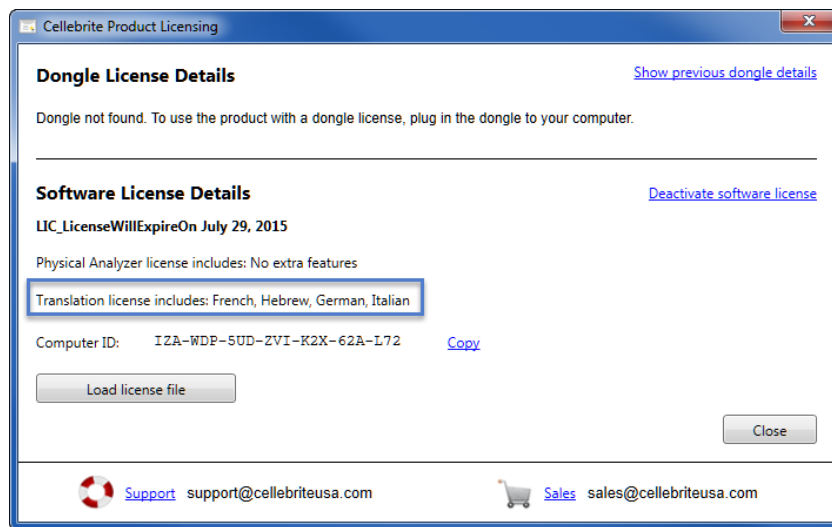
- 5) Update the license for the product and download the language package.

After updating your product license with the selected languages, you can use the following procedure to view the languages included in the translation license.

To view the translation license languages:

- Select **Tools > Translation > Show supported languages**.

The following screen appears.



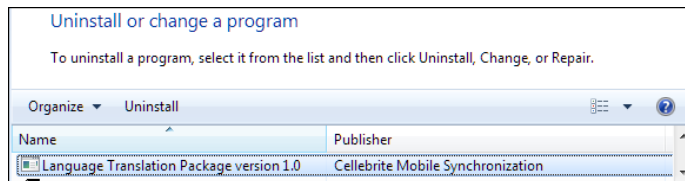
## 6.2.2. Downloading the translation pack

You can download the Translation pack from the application or from your [my.cellebrite.com](http://my.cellebrite.com) account. The Translation pack includes a version number, which enables you to track the version installed on the computer.

To download the translation pack:

- 1) Select **Tools > Translation**.
- 2) Select one of the following options:
  - **Download translation pack:** Downloads the translation pack (this option is not available if there is no Internet connection).
  - **Install translation pack from file:** Installs the translation pack from a file. Select this option if there is no Internet connection.
- 3) Follow the on-screen instructions to install the Translation pack.

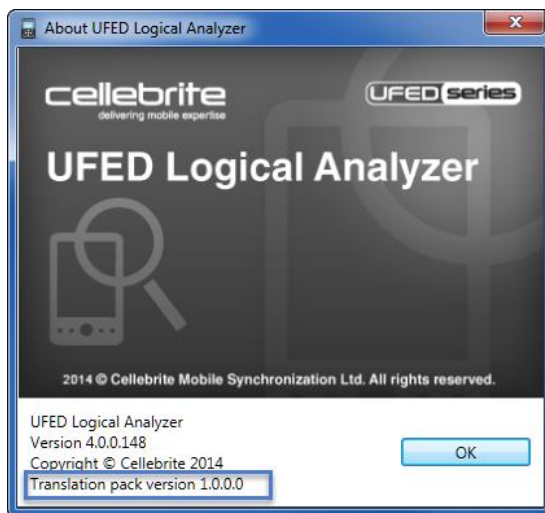
**NOTE:** To uninstall the Translation pack, go to the Windows Uninstall page, and select the Language Translation Package, (Publisher: Cellebrite Mobile Synchronization) from the list.



To view the translation pack version number:

- Click **Help > About**.

The following screen appears.



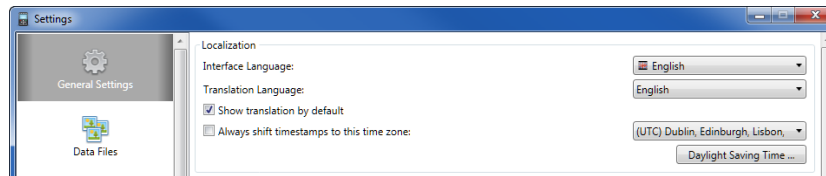
### 6.2.3. Translating the decoded data

By default, the target language is set to the same language as the interface language. If required, you change the target language to a different language.

To change the translation language:

- 1) Select **Tools > Settings**.

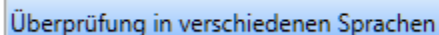
The following screen appears.





- 2) Select the translation language. That is the language to which you want to translate the text. You can only select one target language. To request additional translation languages, select **Get more languages**.
- 3) Select the **Show translation language by default** check box to display translations by default. Clear this check box so that the translation will not appear when you translate text. To see the translation select **View translated**.

To translate decoded data:

- 1) Click to select the data that you want to translate.

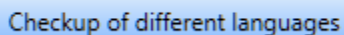


- 2) Click the  button, or right-click and select **Translate selected** or click  and then select one of the following options:

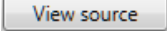
- **Translate all:** Translate all entries in the specified view.
- **Translate selected:** Translate the select text only.

NOTE: If required, use the **Delete translation** option to delete the translated text.

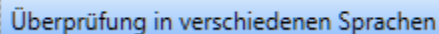
The translated text is indicated by a yellow bar.




To view the original text:

- 3) Right-click the text and select **View source**, or click the  button.

The original text is indicated by with a gray bar.



To filter text:

- Click  and then select one of the following options:
  - **All** to display all text.
  - **Translated** to display text that has been translated.
  - **Not translated** to display text that has not been translated.

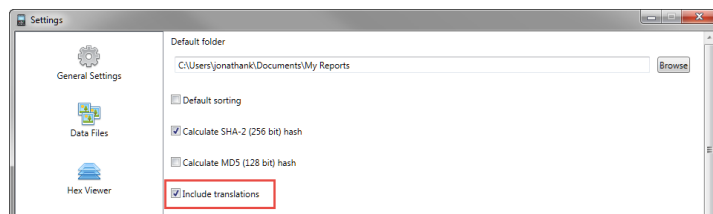
## 6.2.4. Reporting

When creating reports or exporting data, you can specify whether to include the translated text or not. If you choose to display the translated text within the report, the summary table will include an additional entry called: Translated languages, with a list of the languages. The translated content appears below the original text under the heading: Translation. For more information on reports, see [Generating a report](#) on page 119.






To include the translated text in reports:

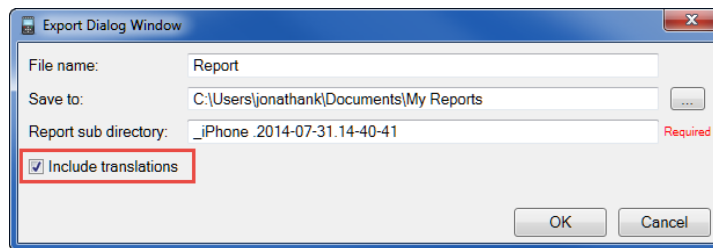
- 1) Go to Tools > Settings > General Settings > Report Defaults.
- 2) Select the **Include translation** check box.





To include translated text in exports:

- 1) Click an Export option (      ).
- 2) Select the **Include translation** check box.





## Chapter 7: Working with project analytics

Project Analytics enables you to view the extraction data in terms of the number of communication events between the device and other parties, identified by phone number, or other user identity (such as email address, Skype handle, and so on). The analysis enables you to easily and efficiently identify communication patterns between the device and other parties. For example:

- Parties most communicated with via all types of communication methods
- Parties most communicated with via phone calls, SMS, and MMS

If the device user exchanged a large number of phone calls, SMS, and emails with a certain contact, it is easy to see the volume of this communication. Communication events are listed by volume per type. The following communication events are supported:

- **Phones** - Lists outgoing, incoming, and missed calls, and sent, received, and draft SMS and MMS.
- **Emails** - Lists emails sent, received, drafts, and emails of unknown status.
- **WhatsApp** - Lists messages sent, received, and drafts.
- **Skype** - Lists calls, SMS, and chat messages.
- **BlackBerry Messenger** - Lists chat messages.

Project analytics runs automatically when you open an extraction file.

To view project analytics:

- 1) Click **+** next to the **Project Analytics** tree item to view the analytics results displayed in the **Project Analytics** tree item.
- 2) Double-click the **Project Analytics** tree item to open a tab that displays the top five activities per contact.
- 3) To view a comparative overview of all communication events, double-click the **Activity Analytics** tree item.

The view is sorted in descending order, based on the total number of events.



- 4) To view the events by communication identifier, double-click the desired identifier tree item.
- 5) Click the column header to sort the information in the column.

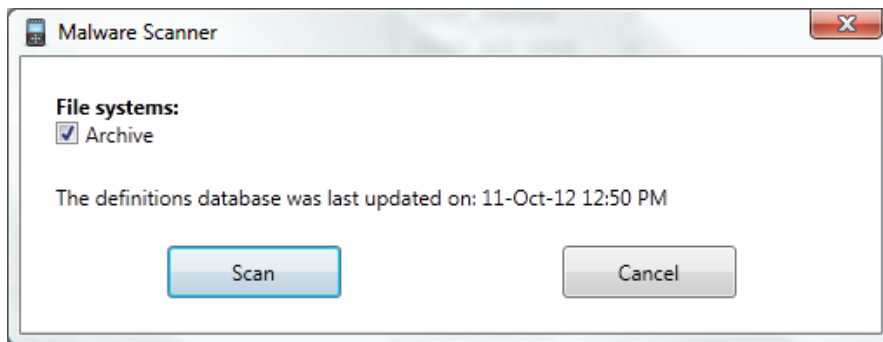
**NOTE:** Project analysis information can be included in a report. For more information, see [Generating a report](#).

## Chapter 8: Scanning for malware

Run malware detection on your extraction to search for malware.

When you scan for malware, UFED Physical Analyzer uses the last-used signature database. If this is the first time you are using the malware scanner, or if you want to update the database before you scan, follow the steps in [Updating the signature database \(online\)](#) (page 110). If you are working on a computer without an internet connection, follow the steps in [Updating the signature database from file \(offline\)](#) (page 112).

- 1) Select **Tools > Malware Scanner > Scan Malware** or click .



- 2) Select the file system(s) that you want to scan, and click **Scan**.

UFED Physical Analyzer scans the project for malware. The results are displayed under the **Malware Scanner** tree item.

- 3) Double-click the **Malware Scanner** tree item to open a data display tab.

The data shown includes the malware type and malware information, such as the name.

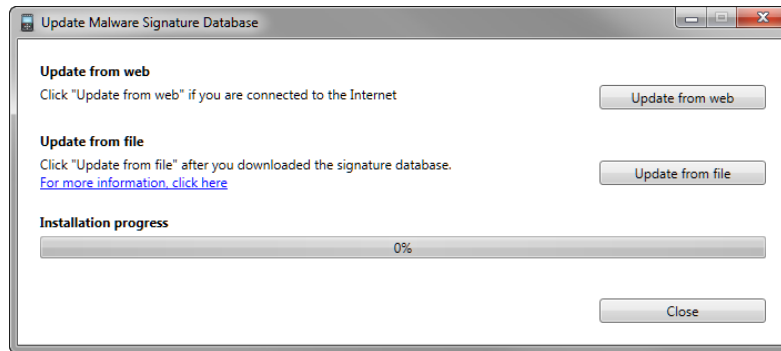
- To include the results in a report, select **Infected Files** in the **Report Dataset** area. For more information, see *Error! Reference source not found.*

## 8.1. Updating the signature database (online)

Update the signature database before the first time you use the malware scanner in order to populate the database, and thereafter in order to keep the signature database up to date.

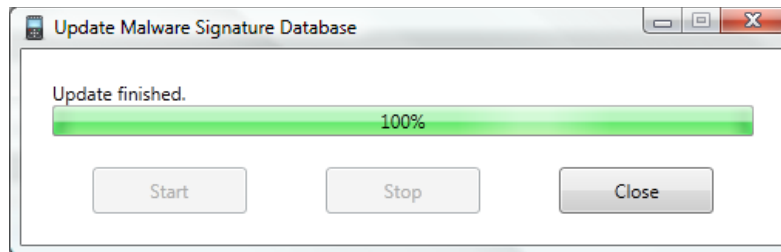
**NOTE:** Once the signature database is populated, you can run the malware scanner using the existing database. It is strongly recommended that you update the signature database on a regular basis in order to keep it current.

- 1) In the **Tools** menu, select **Malware Scanner > Update signature database**.



- 2) Click **Update from server**.

The database is populated.



- 3) Click **Close**.

You can now scan the project for malware.

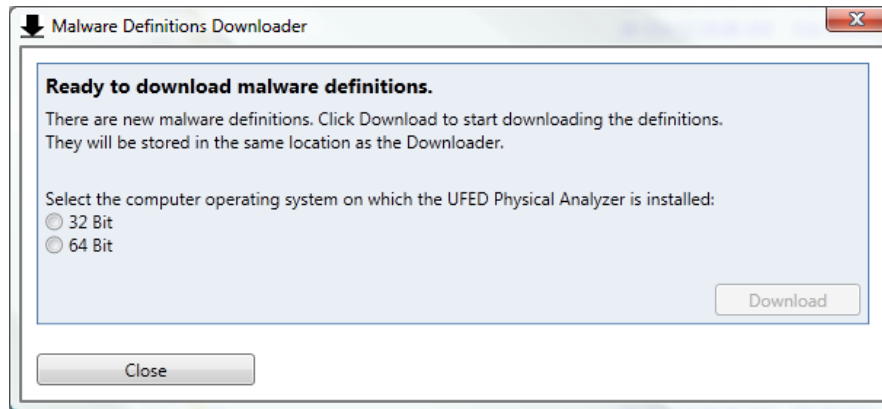
## 8.2. Updating the signature database from file (offline)

Update the signature database from file when you are working on a computer that does not have an internet connection.

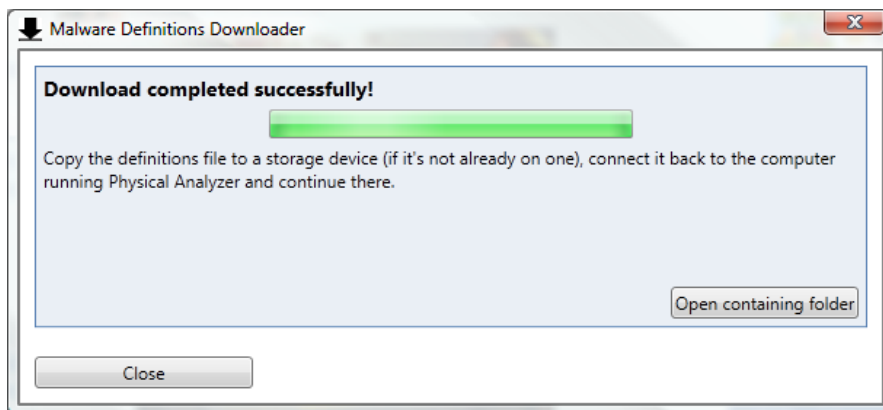
**NOTE:** Once the signature database is populated, you can run the malware scanner using the existing database. It is strongly recommended that you update the signature database on a regular basis in order to keep it current.

- 1) In Windows Explorer, in the main UFED Physical Analyzer directory, copy the **BitDefenderUpdater** directory to an external storage device.
- 2) Transfer the **BitDefenderUpdater** directory to a computer that has internet connection without proxy settings.
- 3) In the **BitDefenderUpdater** directory, double-click **Malware Definitions Downloader.exe**.





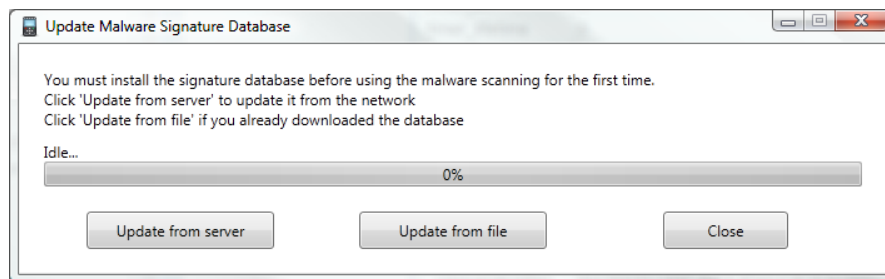
- 4) Select the computer operating system of the computer on which UFED Physical Analyzer is installed.
- 5) Click **Download**.



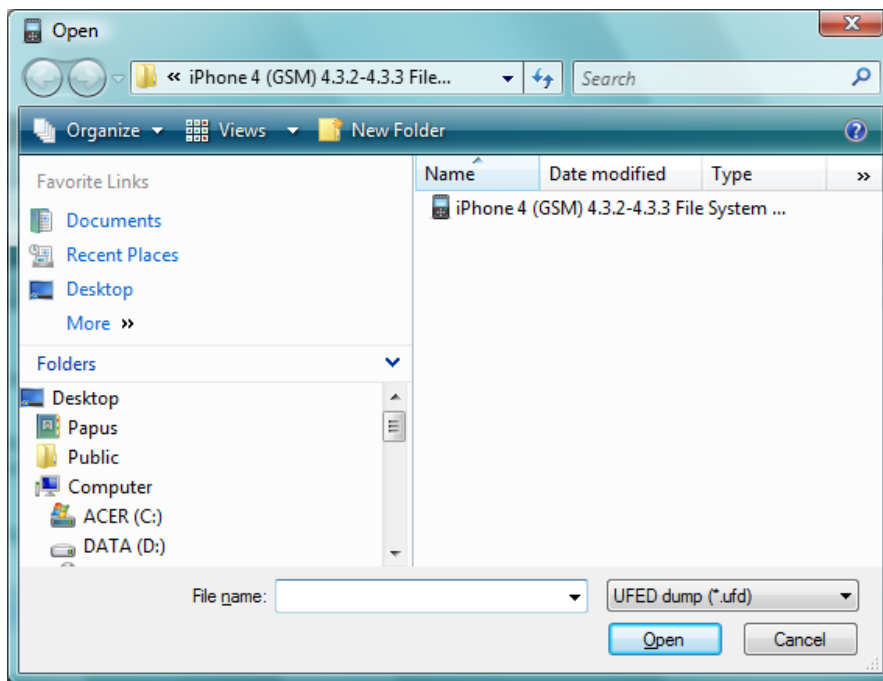
- 6) Click **Open containing folder**.
- 7) Copy the **definitions.msd** file to an external storage device, and transfer it to the computer on which UFED Physical Analyzer is installed.
- 8) Click **Close** to close the Malware Definitions Downloader.

**NOTE:** To streamline your workflow and save time, it is recommended that you always use the same computer to download the **definitions.msd** file. When you download the **definitions.msd** file to this computer in the future, the Malware Definitions Downloader updates the file instead of downloading the entire file. Make sure that you do not delete the **definitions.msd** file from this computer.

- 9) In UFED Physical Analyzer, select **Tools > Malware Scanner > Update signature database**.

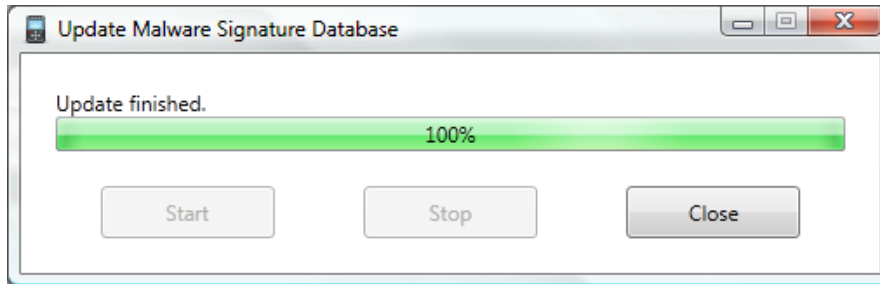


10) Click **Update from file**.



- 11) Browse to the malware definitions database file (\*.msd), and click **Open**.
- 12) Click **Start**.

The database is populated.



- 13) Click **Close**.

You can now scan the project for malware.



## Chapter 9: Generating a report

- 1) You can generate a report of the information in the project. UFED Logical Analyzer provides a report wizard to help you through the steps of creating a report. Do one of the following:
  - Select **Report > Generate Report** from the application menu.
  - Click **Generate Report** in the **Extraction Summary** tab.
  - Double-click **Reports** in the project tree.

The Generate Report window appears.

**Generate Report**

**General**

Report Dataset

\_iPhone 4

Security

Layout

Default sorting

**General**

File name: Report

Save to: C:\Users\jonathank\Documents\My Reports

Report sub directory: 2014-07-31.15-28-58

Project: \_iPhone 4

Format:

**Case Information**

Case number:

Case name:

Evidence number:

Examiner name:

Department:

Location:

Notes:

- 2) In the **File Name**, select the name for the new report you want to create.
- 3) In the **Save to**, select the folder in which you want all reports to be created. This folder can be used for all reporting as each report will occupy a separate sub-folder.
- 4) In the **Report sub-directory** select a name for the folder where you want all selected reports to be created. The default is the current date and time.



- 5) In the **Project** select the project or projects you want to include in this report. Only projects that are already opened in UFED Logical Analyzer are available for reporting.

**Generate Report**

**General**

Report Dataset

\_iPhone 4

\_iPhone 4 #2

Security

Layout

Default sorting

**General**

File name: Report

Save to: C:\Users\jonathank\Documents\My Reports **Browse**

Report sub directory: 2014-07-31.15-32-32

Project: \_iPhone 4; \_iPhone 4 #2

**Format**

☒ \_iPhone 4

☒ \_iPhone 4 #2

**Case Information**

Case number:

Case name:

Evidence number:

**Examiner name:**

Department:

Location:

Notes:

**Close**

**Update settings** **Previous** **Next** **Cancel**

- 6) In the format field choose which of the available formats you want for the report. More than one format can be chosen and a report for each format will be generated.

**Generate Report**

**General**

*Report Dataset*

- \_iPhone 4
- \_iPhone 4 #2

*Security*

*Layout*

- Default sorting
- Word report
- HTML Report
- PDF Report

**General**

File name: Report

Save to: C:\Users\jonathank\Documents\My Reports **Browse**

Report sub directory: 2014-07-31.15-32-32

Project: \_iPhone 4: \_iPhone 4 #2

Format: Word report: HTML Report: PDF Report: XML Report

**Case Information**

Case number:

Case name:

Evidence number:

**Examiner name:**

Department:

Location:

Notes:

☒ Word report

☐ Excel Workbook (xlsx)

☐ Open Document spreadsheet (ods)

☐ Excel 97-2003 (xls)

☒ HTML Report

☒ PDF Report

☐ UFED Report Package

☒ XML Report

**Close**

**Update settings** **Previous** **Next** **Cancel**

7) In the case information fields you can provide the following:

- Case number
- Case name
- Evidence number
- Examiner name
- Department
- Location

NOTE: Default settings for these fields. See *Setting the case information* (page 173). See *Additional report fields* (page 157) and *Report defaults* (page 161) for other defaults. Additionally, the last 10 values entered in these fields is also available in the drop down.

8) Your form should now look like this example:

**Generate Report**

**General**

*Report Dataset*

- \_iPhone 4
- \_iPhone 4 #2

*Security*

*Layout*

- Default sorting
- Word report
- HTML Report
- PDF Report

**General**

File name: Report

Save to: C:\Users\jonathank\Documents\My Reports

Report sub directory: 2014-07-31.15-32-32

Project: \_iPhone 4; \_iPhone 4 #2

Format: Word report; HTML Report; PDF Report; XML Report

**Case Information**

Case number: 1001

Case name: Case 1001

Evidence number: 1001-01-1a

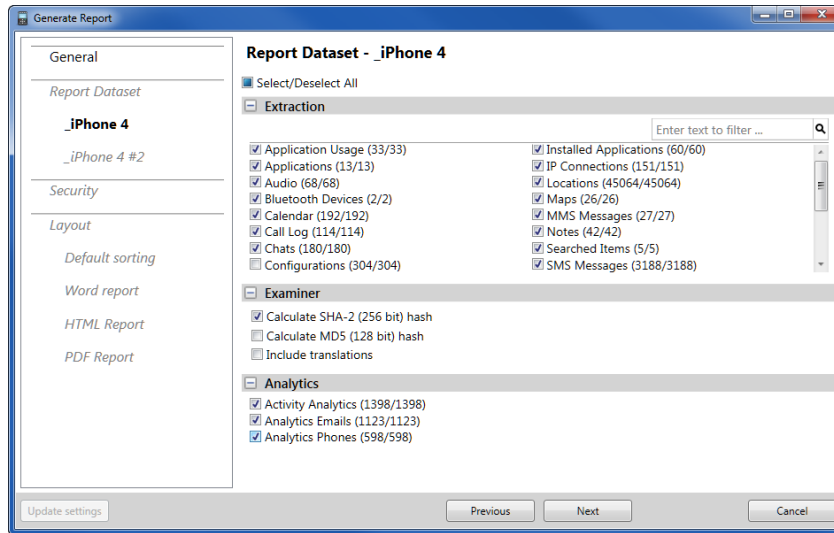
Examiner name: JK

Department: Homicide

Location: NY

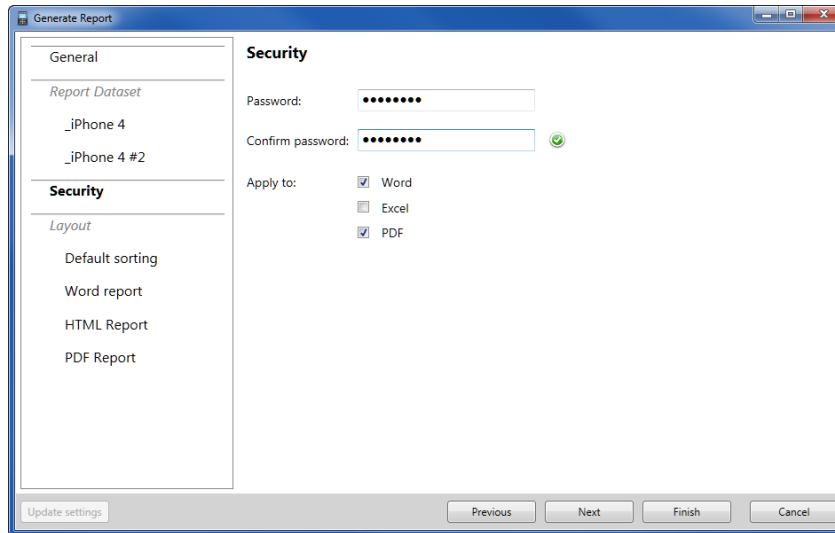
Notes: Case notes for 1001

9) From the following screen select the data to include in the report:



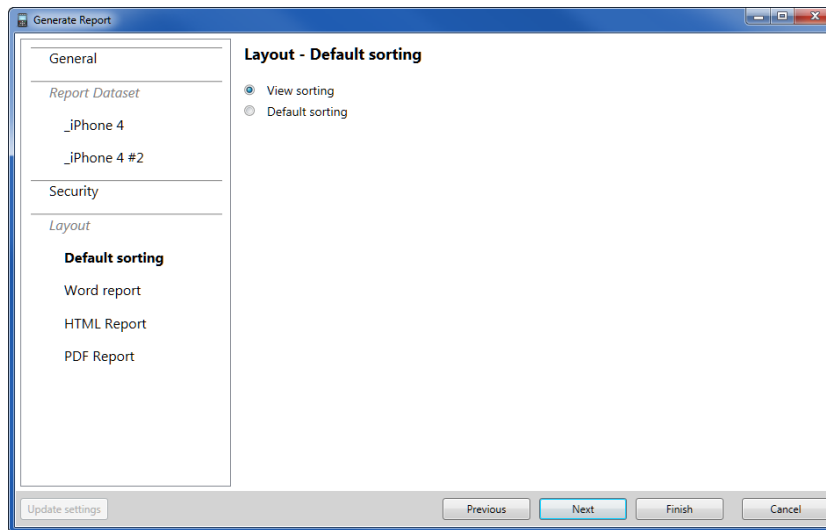
- a) **Extraction** - analyzed data and data files to be included in the report.
- b) **Examiner** - Calculate SHA-2 (256 bit) hash and Calculate MD5 (128 bit hash) - Select which calculated MD5 and SHA256 hash keys to add to each Data Files item in the generated report. This selection is for the whole report and applies to all projects within the report. TIP: To shorten the report generation process of large projects do not select these options.

- c) **Analytics** - this section appears when there is **Analytics** available in the project. Select the relevant Analytics item(s) to include them in the report.
- 10) The **security** screen is presented. Password protection can be put on PDF, WORD and Excel reports:



Choose the format and provide a password.

- 11) Select **Default sorting** to sort the items included in the generated report according to the default sorting set by Cellebrite for each of the Analyzed and Data file types or clear **Default sorting** to sort the items according to the selected sorting field and the sorting order (ascending or descending) that was set by the user in each of the data display tables.



- 12) For each format chosen for this report you can specify report parameters as follows:
- Word, HTML and PDF Reports:

- **Disable models categorization** - Select to disable the separation and generate a report in which every data items is generated as a single section without subcategories separation. By default, a categorized report in which each category in the data items group is generated as a separate section in the report is generated. For example, when generating a report with SMS, select the check box to generate the SMS messages as a single list, or clear the check box to break it to a separate list for each category of SMS messages (Inbox, Outbox, Drafts, etc.).
- **Logo Header** - Text area where you can enter and format custom text to appear in the report header before the logo image.
- **Logo** - Click **Select Image File** to add the logo image to appear in the report header. Supported file formats are: BMP, JPG, GIF, and PNG.
- **Logo Footer** - Enter and format custom text to appear in the report footer after the logo image.
- **Show totals for items not in the report** - Add a **Total** column to the report that displays the total number of items that were excluded from the report.
- **Show extended deleted state** - Include the state (**Intact**, **Deleted**, or **Unknown**) of deleted items in the generated report. When not selected, logs only the state of deleted items as Yes, and is left empty for other states.
- **Number of lines for email preview** - Set the maximum number of lines from each email message to appear in the report.
- **Display full email body** - Display the entire message body.



- **Number of messages per chat** - Set the maximum number of messages per chat message to appear in the report.
- **Display all chat messages** - Display all chat messages in the report.
- **Font Family** - for PDF reports only.
- **Split HTML report** - for HTML reports only. Ensure that each section of the report starts on a new page.

b) Excel (all formats) and ODS report:

- **The excel report is compatible with OpenOffice** - Select to ensure the Excel report can be opened in OpenOffice.
- **Generate Contact Identification Data** - Select to add a sheet to the Excel report that provides a list of unique contacts based on type.

c) XML and UFED Report package:

- There are NO additional settings required for either of these reports. If the report formats requested only include XML and/or UFED report then no further input is required.

13) Click **Finish**.

**NOTE:** **Finish** is unavailable until all the required fields are filled. A yellow warning icon is displayed next to all required fields that are not yet complete.

When the report is successfully generated, you are prompted to open the generated report file. The file opens using the associated application to the file format installed in the workstation.

Once a report has been generated for the project, it can be accessed from the Reports section in the project tree. Double click on any of the generated reports to open it in the associated application installed in the workstation. Right click any of the generated reports to open the report file, or select **Open containing folder** to browse the files and folders of the report.

## Chapter 10: Performing extractions


### 10.1. Performing advanced logical extraction

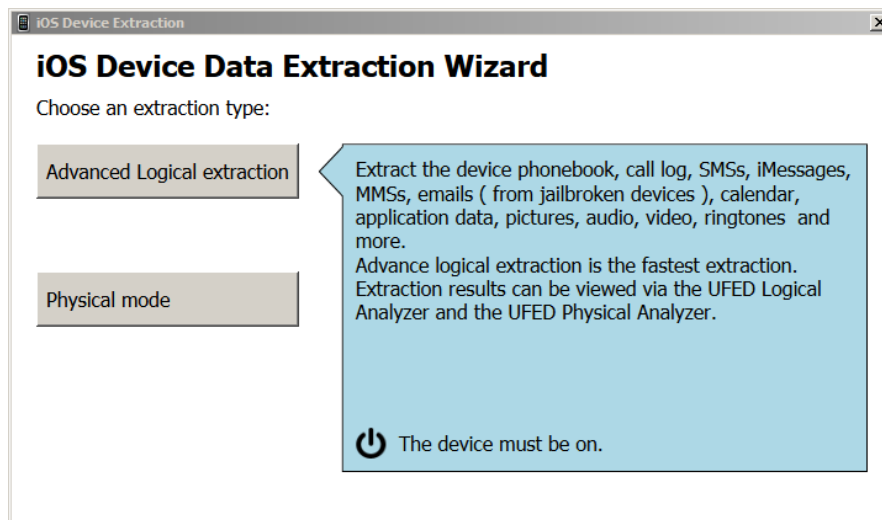
Perform an advanced logical extraction from UFED Logical Analyzer to extract more information than from logical extraction using the UFED unit.

Perform an advanced logical extraction from the following devices:

- iPhone 2G/3G/3GS/4/4s/5/5s/5c
- iPad 1/2/3/4/mini
- iPod Touch 1G/2G/3G/4G
- iPod Nano 5G

### 10.1.1. Performing advanced logical extraction

- 1) Select **Extract > iOS Device Extraction** or click  to start iOS Device Extraction.
- 2) Click **Advanced Logical extraction**.



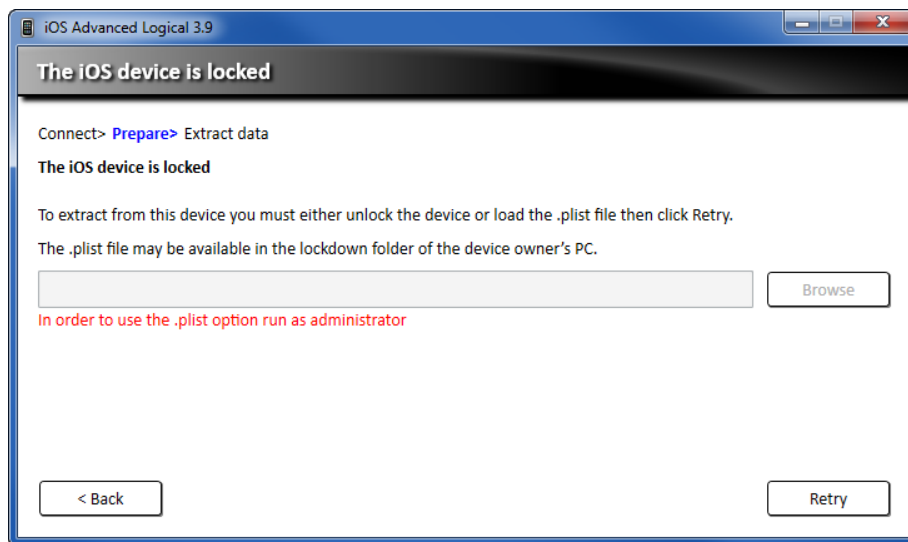
- 3) Follow the displayed instructions to power on the iOS device and connect the device to your computer, then click **Next**.



**NOTE:** If the connected device and not recognized, disconnect the device and reconnect it to a USB port at the rear of the PC.

If the iOS device is locked the **Locked Device** screen is displayed. If the .plist file for the locked device is available from the device owner's PC then this .plist file can be loaded in the **Locked Device** screen and then click **Retry**. If the device is locked and no .plist file is available then click **Close**.

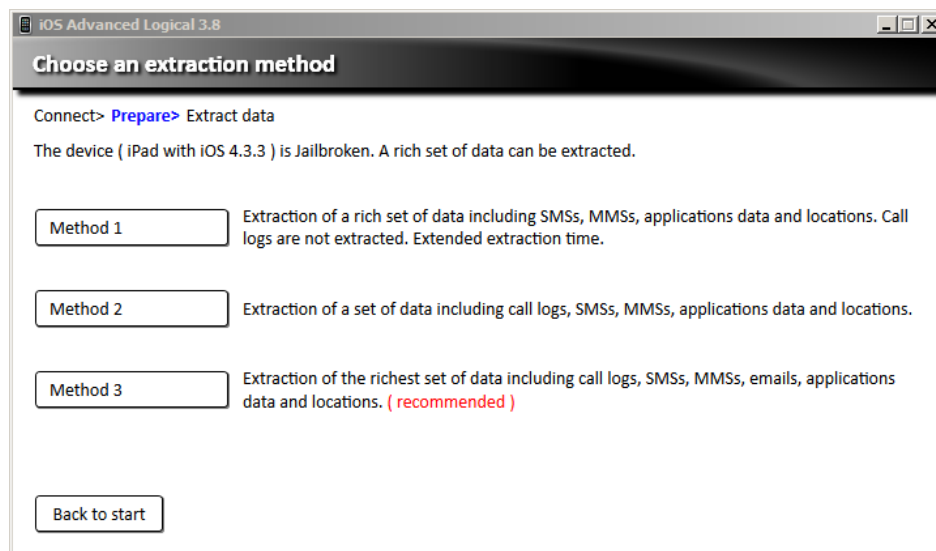
**NOTE:** To use the .plist file, you need to run the UFED application as an administrator.



- 4) Choose a **Method** of Advanced Logical extraction. Depending on whether the device is **jailbroken** and/or **encrypted**, different methods of extraction are made available:
  - a) Method 1 - Extraction of a rich set of data including SMSs, MMSs, application data and locations. Call logs, email body and attachments are not extracted. Extended extraction time.
  - b) Method 2 - Extraction of a set of data including call logs, SMSs, MMSs, application data and locations. This decoding process may require entering the iTunes backup password.
  - c) Method 3 - Extraction of the richest set of data including call logs, SMSs, MMSs, emails, application data and locations.

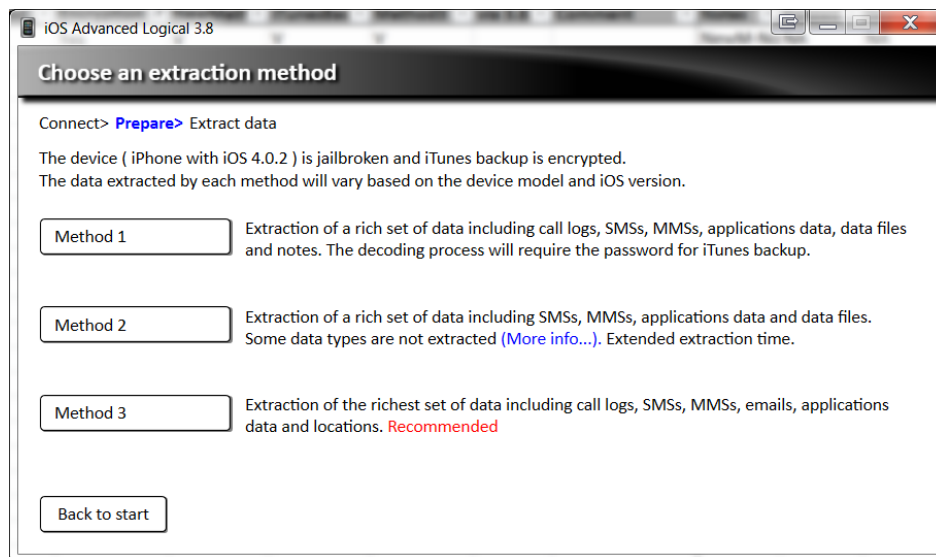
In addition the application indicates a specific recommended method per iTunes backup configuration and jailbroken status.

For a **jailbroken** iOS device this screen is displayed -

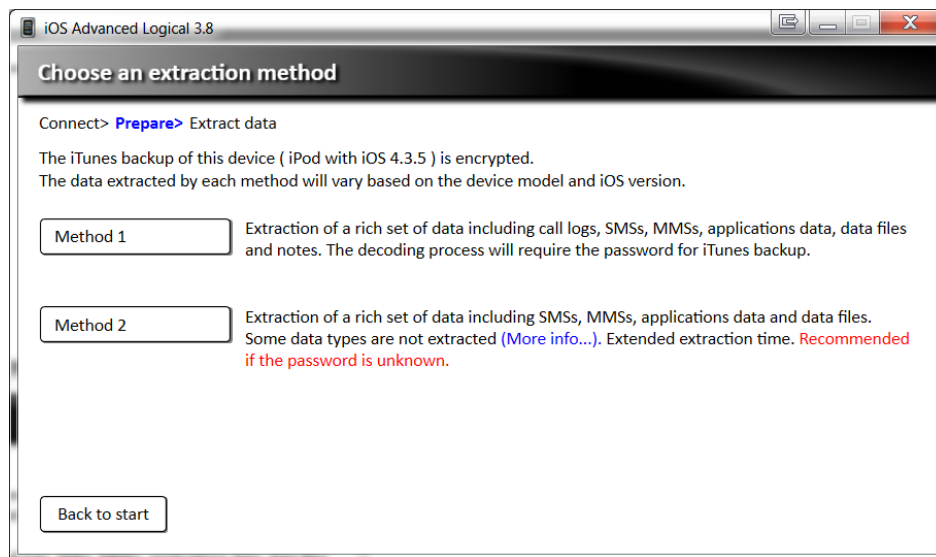




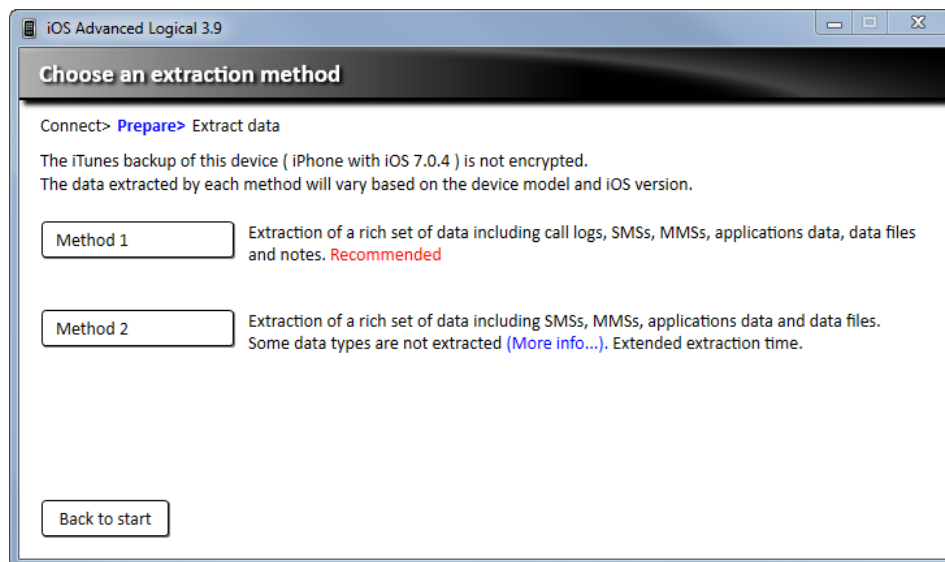
For a **jailbroken encrypted** iOS device this screen is displayed -



For a non-jailbroken encrypted iOS device this screen is displayed -

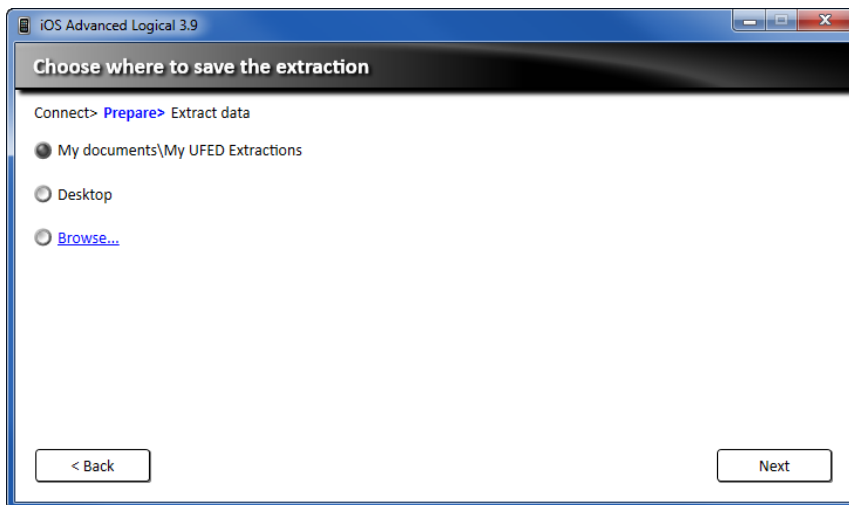


For a non-jailbroken non encrypted iOS this screen is displayed -

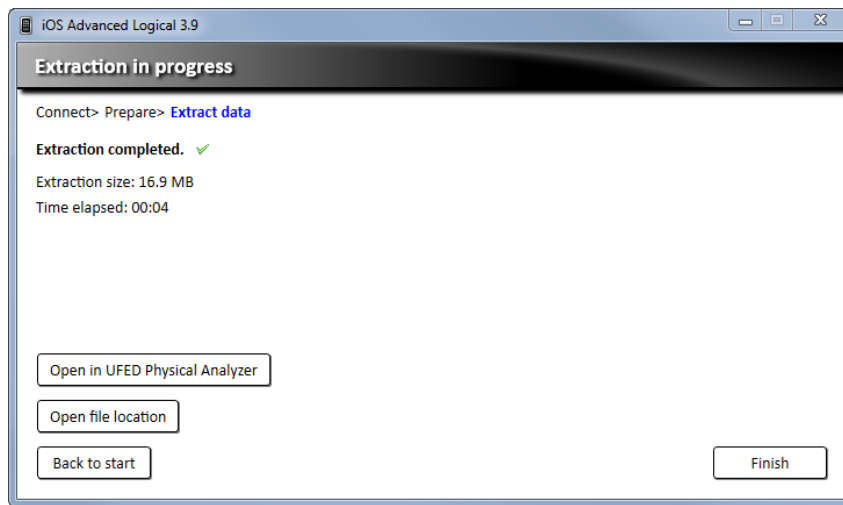


**NOTE:** The extraction time will depend on the amount of data on the iOS device and on the method chosen. A **method2** extraction from a heavily used device could take several HOURS to complete.

- 5) Choose the location to save the extracted data. Ensure that there is enough disk space on your chosen location. You can save it locally on the computer or to any removable storage device or to a network location.



- 6) Click **Next** to continue.
- 7) A progress bar will be shown. Wait for the extraction process to complete.



**NOTE:** The duration varies depending on the extraction method, the device model, the amount of data on the device, the extracting computer, and other parameters.

The advanced logical extraction is saved to the selected location as a \*.UFD file and a \*.TAR file.

Open the advanced logical extraction in UFED Logical Analyzer to access all extracted information.

8) Select one of the following options:

- **Open in UFED Analyzer** – Loads the extraction file in UFED Logical Analyzer.
- **Open file location** – Opens the folder that contains the extraction files.
- **Back to start** – Returns to the extraction methods screen.
- **Finish** – close iOS Device Extraction.

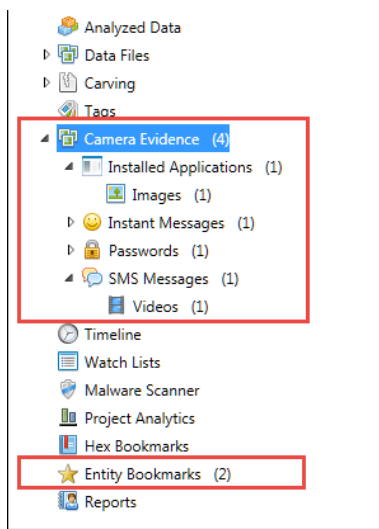
## Chapter 11: Camera and screenshot evidence

UFED 4PC or UFED Touch together with the UFED camera enables you to collect evidence by taking pictures or videos of a device. A screenshot feature captures internal screenshots directly from a Blackberry, Android or iOS device. These options can be useful as complimentary evidence or in instances when data cannot be extracted from a device. This evidence can be displayed in UFED Logical Analyzer together with any notes, categories and bookmarks, which were added by the examiner. For information on capturing camera and screenshot evidence, refer to the *UFED 4PC* or *UFED Touch* user manuals.

### To import camera or screenshot evidence:

- Click the Evidence.ufd file.

The Camera Evidence (pictures and videos) or Phone Evidence (screenshots) is imported into UFED Logical Analyzer as a new project. The evidence includes Phone Evidence or Camera Evidence divided by category, as well as entity bookmarks and notes that were added during the extraction. An example is displayed next.

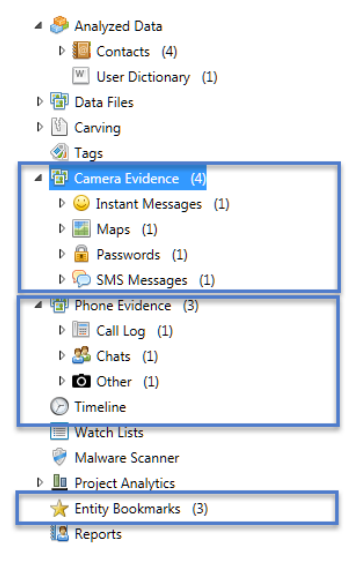




To import camera and screenshot evidence together with the extracted data:

- Click the EvidenceCollection.ufdx file.

The Camera Evidence (pictures and videos), Phone Evidence (screenshots) and the extracted data are imported into UFED Logical Analyzer as a single project. The evidence includes Phone Evidence and Camera evidence, as well as categories, entity bookmarks and notes that were added during the extraction. An example is displayed next.

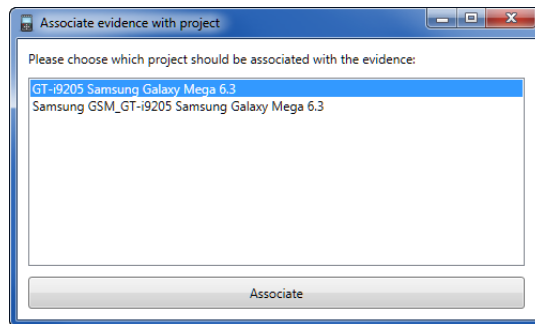


NOTE: Drag-and-drop the EvidenceCollection.ufdx file into UFED Logical Analyzer to open multiple extractions, which were performed for a particular device. That is, all extractions in the folder will be opened. Each extraction (.ufd file) in the folder can also be opened individually. An example folder with multiple extractions and a UFDX file is displayed next.



To associate camera and screenshot evidence with an extraction type:

If you have multiple extraction types as well as camera evidence, the Associate evidence with project screen appears.




- Select the required extraction and click **Associate**.

## Chapter 12: Settings

The Settings window provides a set of functional and behavioral setup options used to fine-tune and control the functionality and usability of the application. The settings in the Settings window apply to all the projects open in UFED Logical Analyzer.

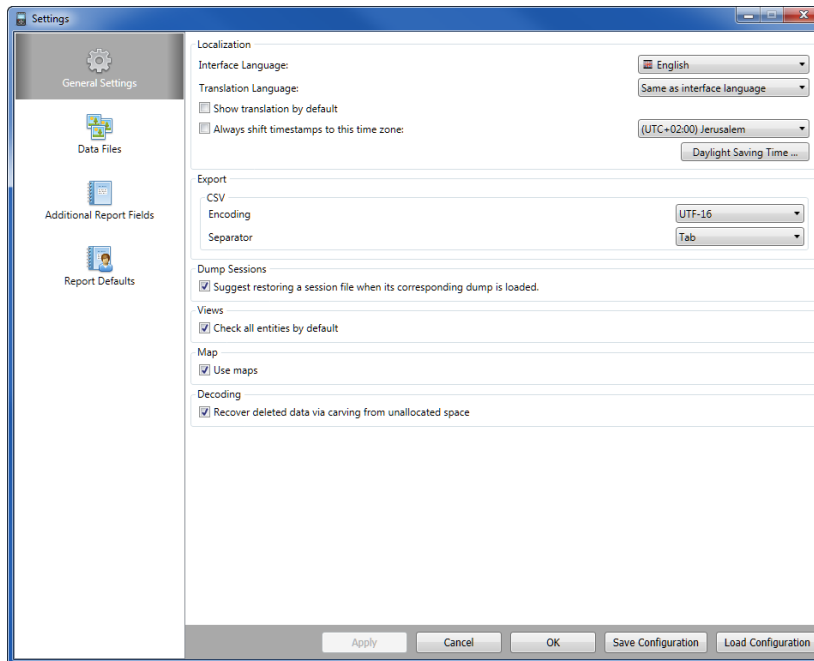
**NOTE:** Changes to settings are lost when you close UFED Logical Analyzer. To save the settings configuration, see [Saving settings](#) (page 169).

- To access the Settings window, do one of the following:
  - Select **Tools > Settings**.
  - Click .

The Settings window appears.

## 12.1. General settings

Set general application settings in the General Settings tab.



To set the interface language of UFED Logical Analyzer:

- In the **Language** list, select the desired language.

To set the translation language:

- Select the Translation Language. That is the language to which you want to translate the text. You can only select one Translation Language. To request additional translation languages, select **Get more languages**.
- Select the **Show translation language by default** check box to display translations by default. Clear this check box so that the translation will not appear when you translate text. To see the translation select **View translated**.

To shift timestamps to a particular time zone:

- 1) From the Time zone settings (UTC) list, select:
  - Original UTC value to show time stamps as recorded (without unification)
  - One of the time zones (UTC -12:00 to UTC +13:00) to recalculate network-defined time stamps according to the time zone offset.
- 2) To change the start and end dates for daylight saving time, click **Daylight Saving Time**. For more information on how to change the time zone settings, *see [Setting a unified time zone for the project](#)* (page 170).

To set the encoding and separator of exported CSV files:

- 1) In the **Export** area, select the desired encoding option from the **Encoding** list.
- 2) Select the desired separator in the **Separator** list.

To set UFED Logical Analyzer to automatically verify images on project load:

- Select **Automatically verify images on project load**.

To have UFED Logical Analyzer offer to load a session when opening its corresponding extraction:

- Select **Suggest restoring a session file when its corresponding dump is loaded**.

To select all entities in all views by default:

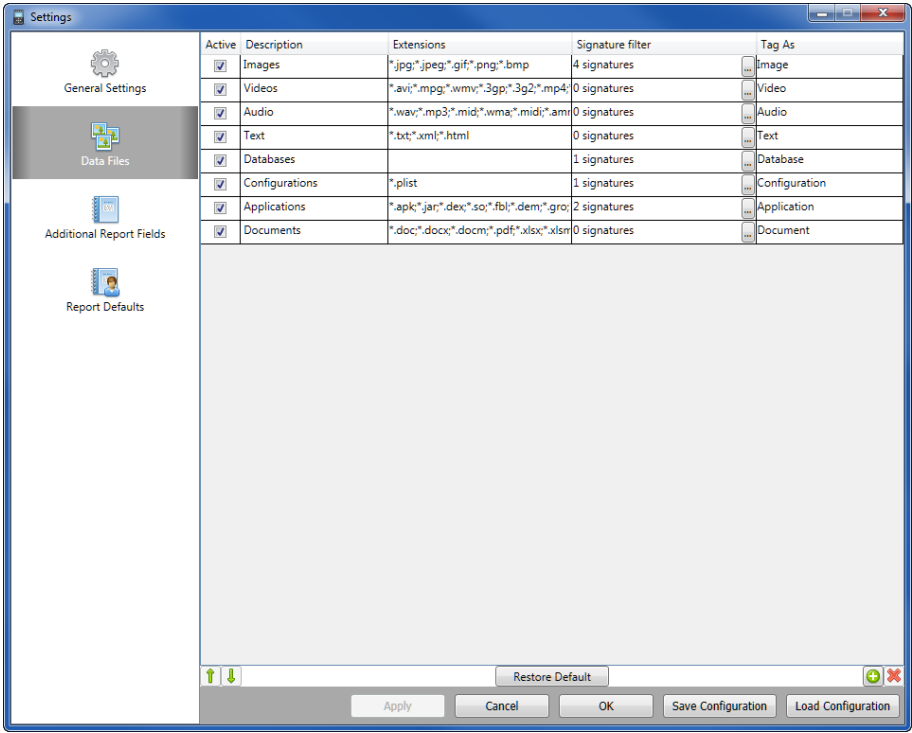
- Select **Check all entities by default**.

Selected entities are included in reports that you generate.

To determine the number of digits required for phone number uniqueness:

- In the **Analytics** area, select the desired number of digits from the **Number of digits to determine phone number uniqueness**.

12.2. Data files



The **Data Files** settings determine the different file and tagging groups under the **Data Files** and **Tags** tree items, and the types of files filtered in each group.

Every data file record contains the following settings:

- **Active** - Indicates whether to display (checked) or hide (unchecked) this group of data files in the project tree.
- **Description** - A descriptive name for the type of data files to be used as the group name under the **Data files** tree item.
- **Extensions** - The file extensions to be used to filter the data files of this group.
- **Signature filter** - The header and/or footer signatures to be used to filter the data files of this group.
- **Tag As** - The tag name to be applied to the data file and used to list the files under **Tags** in the project tree.



### 12.2.1. Data files filtering methods

Groups can be filtered using one or more of the following methods:

- Signature filter

A signature filter is a definition of the file header and/or footer to be searched, in order to detect a file type and associate it with a specific Data File group. The header and/or footer can be configured in a defined range from the beginning and end of the file respectively by using the offset parameter.

For example, a JPEG image starts with the header FF D8 FF and ends with the footer FF D9. Entering this information in the Header and Footer fields of the signature creates a signature that identifies JPEG images.

- Extension filter

An extension filter is a list of common file extensions that are associated with file formats that belong to the specific data file group.

For example, the different image file formats can be filtered by the file extensions \*.jpg, \*.jpeg, \*.gif, \*.png or \*.bmp.

## 12.2.2. Managing data files settings

Add new types of data files, and edit and delete existing data file types.

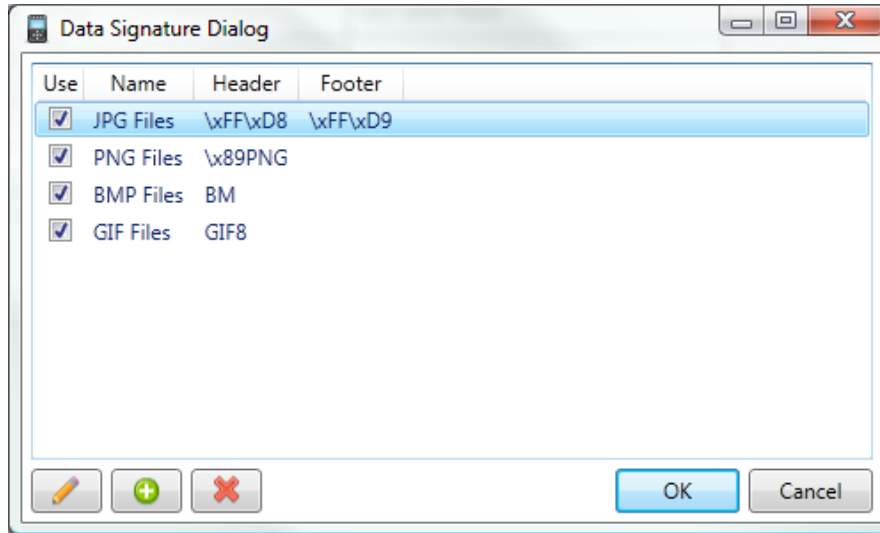
### 12.2.2.1. Adding a new data file type




- 1) In the **Data Files** settings, click .


A new row is added to the list.

- 2) Select **Active** to display the added data type in the **Data Type** tree item.
- 3) Click in the new row's **Description** box, and type a file type description.
- 4) If applicable, in the **Extensions** box, enter the file extensions commonly used by your data file type in the format **\*.xxx**, and separated by **;**.

5) If applicable, in the **Signature filter** box, click  and do any of the following:




- Click  to add a filtering signature that identifies your data file type.
- Click  to edit an existing signature filter.
- Click  to delete a signature filter.

- 6) If applicable, click in the **Tag As** box, click and select a tag name from the list.
- 7) To change the order of the data file types, use the arrows .
- 8) To clear the list of data file types you added, leaving only the default types, click **Restore default**.

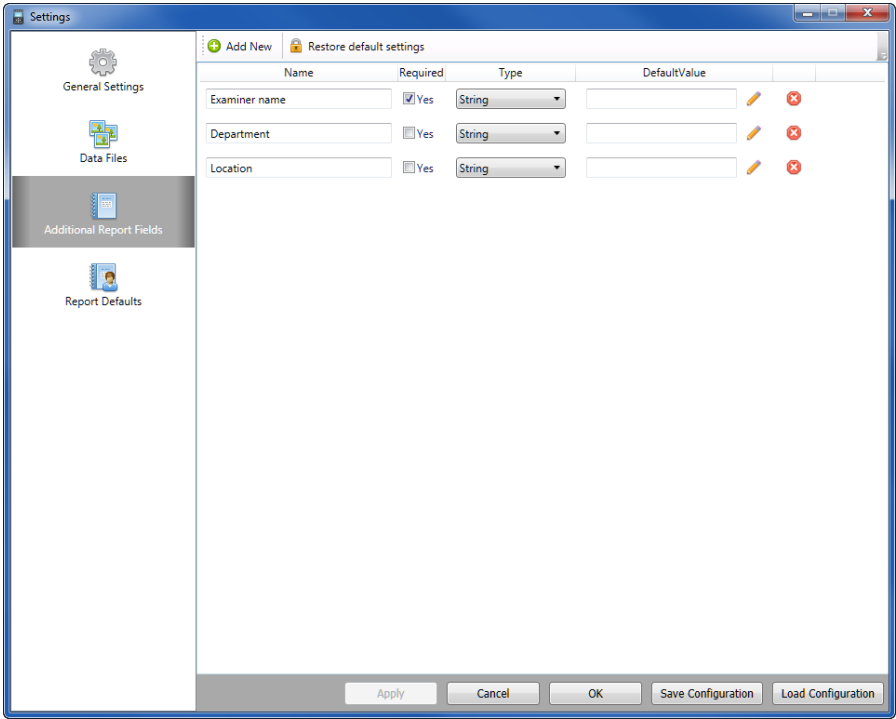
#### **12.2.2.2. Editing an existing data file record**

- 1) Click the row of the data file type that you want to edit.
- 2) Double-click in the column and row that you want to change, and update the existing settings as desired.

#### **12.2.2.3. Deleting a data file type**

- 1) Click the row of the data file type that you want to delete.
- 2) Click .

### 12.3. Additional report fields



Optional information is user-defined information presented at the beginning of the report. It usually includes information about the case, investigator, and organization details.

Every optional information record consists of the following:

<b>Name</b>	The name of the report field.
<b>Required</b>	Indicates if the field must be filled in order to generate the report
<b>Type</b>	The types of entry - <b>String</b> or <b>List</b> .
<b>Default value</b>	Default content.


You can add new report fields, and edit and delete fields, as desired.

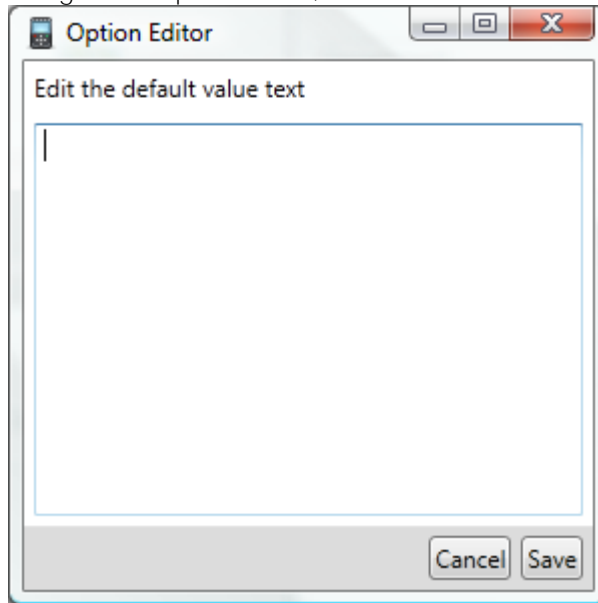
### 12.3.1. Adding a new report field


- 1) Click **Add New**.

A new row is added to the table.

- 2) In the **Name** column, enter the name label to be displayed.
- 3) Select **Required** if this field must be filled in order for the user to generate the report.
- 4) In the **Type** list, select one of the following:
  - **String** for text entry fields
  - **List** for a specified list of options
- 5) In the **Default Value** box, set the default content:

- For **String** type, type the default string. For a multi-line string, click , enter the default string in the Option Editor, then click **Save**.



- For a **List** type, click , enter the list items with each item on a separate line, then click **Save**.

### 12.3.2. Deleting a report field

- To delete a report field, click .

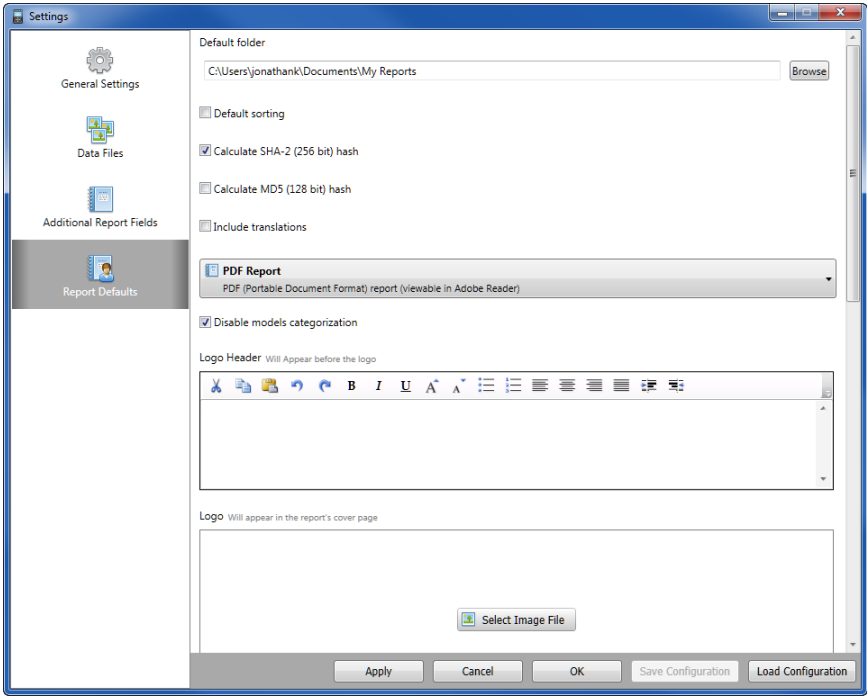
### 12.3.3. Editing a report field

- To edit a report field, perform steps 2-5 of *Adding a new report field* (page 158), changing the parameters to suit your needs.



# 12.4. Report defaults

The Report Defaults settings enable you to edit the report presentation.



NOTE: Scroll down to see all the fields.

1) In the **Report type** list, select the report type that you want to edit.

2) For Excel reports, set the following:

- **Default folder** - enter the path to the folder where you want to save reports you generate for this report type.
- Select **Default sorting** to set sort the items included in the generated report according to the default sorting set by Cellebrite for each of the Analyzed and Data file types or clear **Default sorting** to sort the items according to the selected sorting field and the sorting order (ascending or descending) that was set by the user in each of the data display tables.
- **Calculate SHA-2 (256 bit) hash** and **Calculate MD5 (128 bit hash)** - Select which calculated MD5 and SHA256 hash keys to add to each Data Files item in the generated report. Do not select these options to shorten the report generation process of large projects.
- **Include translations** – **Select to include any translated text in the report.**
- **Unprintable characters placeholder** - Set the placeholder character to replace the unprintable characters.
- **Output File Format** - Set the output file format of the spreadsheet file to either:
  - \* **XLSX** - The current Excel file format.
  - \* **XLS** - The legacy file format of Excel.
  - \* **ODS** - The spread file format of OpenOffice.
- **The excel report is compatible with OpenOffice** - Select to ensure the Excel report can be opened in OpenOffice.

- **Generate Contact Identification Data** - Select to add a sheet to the Excel report that provides a list of unique contacts based on type.
- 3) For HTML reports, set the following:
- **Default folder** - enter the path to the folder where you want to save reports you generate for this report type.
  - Select **Default sorting** to set sort the items included in the generated report according to the default sorting set by Cellebrite for each of the Analyzed and Data file types or clear **Default sorting** to sort the items according to the selected sorting field and the sorting order (ascending or descending) that was set by the user in each of the data display tables.
  - **Calculate SHA-2 (256 bit) hash** and **Calculate MD5 (128 bit hash)** - Select which calculated MD5 and SHA256 hash keys to add to each Data Files item in the generated report. Do not select these options to shorten the report generation process of large projects.
  - **Include translations** – Select to include any translated text in the report.
  - **Disable models categorization** - select to disable the separation and generate a report in which every data items is generated as a single section without subcategories separation. By default, a categorized report in which each category in the data items group is generated as a separate section in the report is generated. For example, when generating a report with SMS, select the check box to generate the SMS messages as a single list, or clear the check box to break it to a separate list for each category of SMS messages (Inbox, Outbox, Drafts, etc.).
  - **Logo Header** - Enter and format custom text to appear in the report header before the logo image.

- **Logo** - Click **Select Image File** to add the logo image to appear in the report header. Supported file formats are: BMP, JPG, GIF, and PNG.
  - **Logo Footer** - Enter and format custom text to appear in the report footer after the logo image.
  - **Show totals for items not in the report** - Add a **Total** column to the report that displays the total number of items that were excluded from the report.
  - **Show extended deleted state** - Include the state (**Intact**, **Deleted**, or **Unknown**) of deleted items in the generated report. When not selected, logs only the state of deleted items as Yes, and is left empty for other states.
  - **Number of lines for email preview** - Set the maximum number of lines from each email message to appear in the report.
  - **Display full email body** - Display the entire message body.
  - **Number of messages per chat** - Set the maximum number of lines per chat message to appear in the report.
  - **Display all chat messages** - Display all chat messages in the report.
  - **Split HTML report** - Set each section of the report to start on a new page.
- 4) For PDF reports, set the following:
- **Default folder** - enter the path to the folder where you want to save reports you generate for this report type.
  - Select **Default sorting** to set sort the items included in the generated report according to the default sorting set by Cellebrite for each of the Analyzed and Data file types or clear **Default sorting** to sort the items according to the selected sorting field and the sorting order (ascending or descending) that was set by the user in each of the data display tables.

- **Calculate SHA-2 (256 bit) hash and Calculate MD5 (128 bit hash)** - Select which calculated MD5 and SHA256 hash keys to add to each Data Files item in the generated report. Do not select these options to shorten the report generation process of large projects.
- **Include translations** – Select to include any translated text in the report.
- **Disable models categorization** - select to disable the separation and generate a report in which every data items is generated as a single section without subcategories separation. By default, a categorized report in which each category in the data items group is generated as a separate section in the report is generated. For example, when generating a report with SMS, select the check box to generate the SMS messages as a single list, or clear the check box to break it to a separate list for each category of SMS messages (Inbox, Outbox, Drafts, etc.).
- **Logo Header** - Enter and format custom text to appear in the report header before the logo image.
- **Logo** - Click **Select Image File** to add the logo image to appear in the report header. Supported file formats are: BMP, JPG, GIF, and PNG.
- **Logo Footer** - Enter and format custom text to appear in the report footer after the logo image.
- **Show totals for items not in the report** - Add a **Total** column to the report that displays the total number of items that were excluded from the report.
- **Show extended deleted state** - Include the state (**Intact**, **Deleted**, or **Unknown**) of deleted items in the generated report. When not selected, logs only the state of deleted items as Yes, and is left empty for other states.

- **Number of lines for email preview** - Set the maximum number of lines from each email message to appear in the report.
  - **Display full email body** - Display the entire message body.
  - **Number of messages per chat** - Set the maximum number of lines per chat message to appear in the report.
  - **Display all chat messages** - Display all chat messages in the report.
- 5) For UFED report packages, set the following:
- **Default folder** - enter the path to the folder where you want to save reports you generate for this report type.
  - Select **Default sorting** to set sort the items included in the generated report according to the default sorting set by Cellebrite for each of the Analyzed and Data file types or clear **Default sorting** to sort the items according to the selected sorting field and the sorting order (ascending or descending) that was set by the user in each of the data display tables.
  - **Calculate SHA-2 (256 bit) hash** and **Calculate MD5 (128 bit hash)** - Select which calculated MD5 and SHA256 hash keys to add to each Data Files item in the generated report. Do not select these options to shorten the report generation process of large projects.
- 6) For Word reports, set the following:
- **Default folder** - enter the path to the folder where you want to save reports you generate for this report type.
  - Select **Default sorting** to set sort the items included in the generated report according to the default sorting set by Cellebrite for each of the Analyzed and Data file types or clear

**Default sorting** to sort the items according to the selected sorting field and the sorting order (ascending or descending) that was set by the user in each of the data display tables.

- **Calculate SHA-2 (256 bit) hash** and **Calculate MD5 (128 bit hash)** - Select which calculated MD5 and SHA256 hash keys to add to each Data Files item in the generated report. Do not select these options to shorten the report generation process of large projects.
- **Include translations** – Select to include any translated text in the report.
- **Disable models categorization** - Select to disable the separation and generate a report in which every data items is generated as a single section without subcategories separation. By default, a categorized report in which each category in the data items group is generated as a separate section in the report is generated. For example, when generating a report with SMS, select the check box to generate the SMS messages as a single list, or clear the check box to break it to a separate list for each category of SMS messages (Inbox, Outbox, Drafts, etc.).
- **Logo Header** - Enter and format custom text to appear in the report header before the logo image.
- **Logo** - Click **Select Image File** to add the logo image to appear in the report header. Supported file formats are: BMP, JPG, GIF, and PNG.
- **Logo Footer** - Enter and format custom text to appear in the report footer after the logo image.
- **Show totals for items not in the report** - Add a **Total** column to the report that displays the total number of items that were excluded from the report.

- **Show extended deleted state** - Include the state (**Intact**, **Deleted**, or **Unknown**) of deleted items in the generated report. When not selected, logs only the state of deleted items as Yes, and is left empty for other states.
- **Number of lines for email preview** - Set the maximum number of lines from each email message to appear in the report. The report includes links to text files containing the entire email.
- **Display full email body** - Set to display the entire message body.
- **Number of messages per chat** - Set the maximum number of lines per chat message to appear in the report.
- **Display all chat messages** - Display all chat messages in the report.

7) For XML reports, set the following:

- **Default folder** - enter the path to the folder where you want to save reports you generate for this report type.
- Select **Default sorting** to set sort the items included in the generated report according to the default sorting set by Cellebrite for each of the Analyzed and Data file types or clear **Default sorting** to sort the items according to the selected sorting field and the sorting order (ascending or descending) that was set by the user in each of the data display tables.
- **Calculate SHA-2 (256 bit) hash** and **Calculate MD5 (128 bit hash)** - Select which calculated MD5 and SHA256 hash keys to add to each Data Files item in the generated report. Do not select these options to shorten the report generation process of large projects.
- **Include translations** – Select to include any translated text in the report.



## 12.5. Saving settings

Save your settings to reuse later, or to share with another user.

- 1) In the Settings window, click **Save Configuration**.
- 2) In the Save As window, browse to the location where you want to save your settings configuration, and click **Save**.

The settings are saved as a UFED Logical Analyzer Settings Configuration File (\*.cnf).

## 12.6. Loading settings

Load your saved settings configuration.

- 1) In the Settings window, click **Load Configuration**.
- 2) In the Open window, browse to the location where your settings configuration is saved, select the configuration (\*.cnf), and click **Open**.

The settings are applied in the Settings window.

## 12.7. Setting project settings

Set unified time zone and case information for each project.

### 12.7.1. Setting a unified time zone for the project

During extraction, one time stamp per event is extracted.

For outgoing events, the time stamp is typically taken from one of the following sources:

- User-defined device time (where the device time has been manually set by the user: timestamps are displayed without the unified time (UTC).
- Network-defined device time (where the device time is automatically set by the network): timestamps are displayed with the unified time (UTC).

For incoming events, the time stamp is typically taken from the network-defined time (the time stamp assigned by the network); timestamps are displayed with the unified time (UTC).

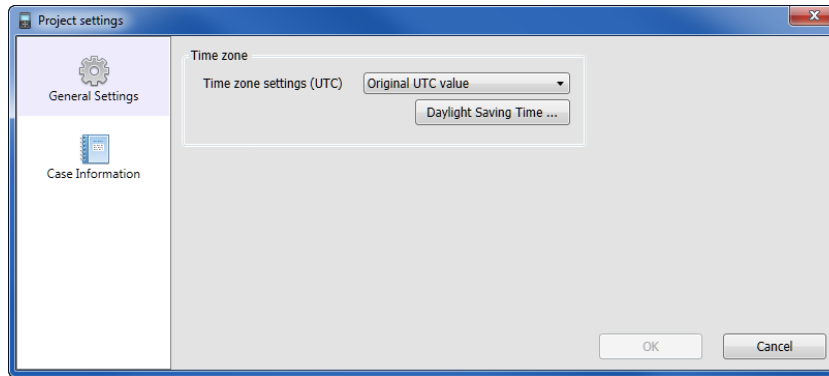
Network-defined time stamps are subject to the time zones in which the event occurred.

Apply a unified time zone to the project to recalculate all network-defined time stamps according to the selected time zone in order to consolidate the events and view them sequentially in UFED Logical Analyzer.

**To apply a unified time zone to the project:**

- 1) Do one of the following:
  - In the project **Extraction Summary** tab, click **Project settings**.

- Click .



- 2) From the **Time zone settings (UTC)** list, select:
- **Original UTC value** to show time stamps as recorded (without unification)
  - One of the time zones (**UTC -12:00** to **UTC +13:00**) to recalculate network-defined time stamps according to the time zone offset.


**NOTE:** User-defined time stamps are not included in these recalculations, and are displayed as recorded.

3) To change the start and end dates for daylight saving time, click **Daylight Saving Time**.

The dialog box is titled "Daylight Savings" and has a dropdown menu set to "(UTC+00:00) London". It contains two columns of data: "Start" and "End". Each row represents a year from 2008 to 2018. The "Start" column shows the date and time (01:00) for the start of daylight saving time. The "End" column shows the date and time (01:00) for the end of daylight saving time. A red 'X' is present in the rightmost column of each row, indicating a missing or invalid end date. At the bottom, there are buttons for "Back to last saved data", "Back to original data", "Save", and "Cancel".

	Start	End	
2018	March, 25, 2018 01:00	October, 28, 2018 01:00	X
2017	March, 26, 2017 01:00	October, 29, 2017 01:00	X
2016	March, 27, 2016 01:00	October, 30, 2016 01:00	X
2015	March, 29, 2015 01:00	October, 25, 2015 01:00	X
2014	March, 30, 2014 01:00	October, 26, 2014 01:00	X
2013	March, 31, 2013 01:00	October, 27, 2013 01:00	X
2012	March, 25, 2012 01:00	October, 28, 2012 01:00	X
2011	March, 27, 2011 01:00	October, 30, 2011 01:00	X
2010	March, 28, 2010 01:00	October, 31, 2010 01:00	X
2009	March, 29, 2009 01:00	October, 25, 2009 01:00	X
2008	March, 30, 2008 01:00	October, 26, 2008 01:00	X

Back to last saved data    Back to original data    Save    Cancel

- a) For the year that you want to change, use the calendar to select the start and end dates, or edit the dates directly. You can use the  button to remove certain years.
  - b) Click **Back to last saved data** to reset the table to the last time that you saved the data, click **Back to original data** to return the table to its default settings, or click **Save** to save the table with any changes that you made.
- 4) Click **OK**.

The project is recalculated according to the selected unified time zone, and the new time zone is applied to the network-defined time stamps. Time stamps of events displayed in UFED Logical Analyzer windows and any subsequently-generated reports reflect the selected unified time zone.

### 12.7.2. Setting the case information

Case information settings are saved with the project. The case number appears with the extraction information on the Welcome tab.

- 1) Do one of the following:
  - In the project **Extraction Summary** tab, click **Project settings**.
  - Click .

2) Click **Case Information**.

The screenshot shows the 'Project settings' dialog box with the 'Case Information' tab selected. The dialog has a sidebar on the left with 'General Settings' and 'Case Information' (selected). The main area contains a table with columns: Name, Required, Type, and DefaultValue. There are four rows of settings: Case number, Case name, Evidence number, and Notes. Each row has a text input field, a 'Required' checkbox (all are checked), a 'Type' dropdown menu (all are set to 'String'), and a 'DefaultValue' text input field with an edit icon. At the top of the main area are buttons for 'Add New' and 'Restore default settings'. At the bottom are 'OK' and 'Cancel' buttons.




Name	Required	Type	DefaultValue
Case number	<input checked="" type="checkbox"/> Yes	String	
Case name	<input checked="" type="checkbox"/> Yes	String	
Evidence number	<input checked="" type="checkbox"/> Yes	String	
Notes	<input checked="" type="checkbox"/> Yes	String	

3) Click **Add New**.

Some case information fields appear by default.

4) Set the parameters for the default information fields:

- In the **Name** column, enter the relevant information (for example, case number, name, or notes).
- Select **Required** if this field must be filled.
- In the **Type** list, select one of the following:
  - **String** for text entry fields

- **List** for a specified list of options
- d) In the **Default Value** box, set the default content:
- For **String** type, type the default string. For a multi-line string, click , enter the default string in the Option Editor, then click **OK**.
  - For a **List** type, click , enter the list items with each item on a separate line, then click **OK**.
- 5) To add more information fields, click **Add New**, and repeat step 3.
- 6) To remove the custom entries, click .
- 7) To restore the default settings, click **Restore default settings**.





## Chapter 13: Reference

### 13.1. File menu

Open	Open a file for analysis using the standard analysis process.
Recent	Displays a list of recent projects.
Close	Closes the currently active project
Save Project Session	Saves the active project information generated by the user as a UFED Logical Analyzer session file (*.pas). See Saving a project session.
Load Project Session	Loads a UFED Logical Analyzer session file (*.pas) onto an open project in the project tree.
Exit	Closes the UFED Logical Analyzer and all active sessions.

### 13.2. View menu

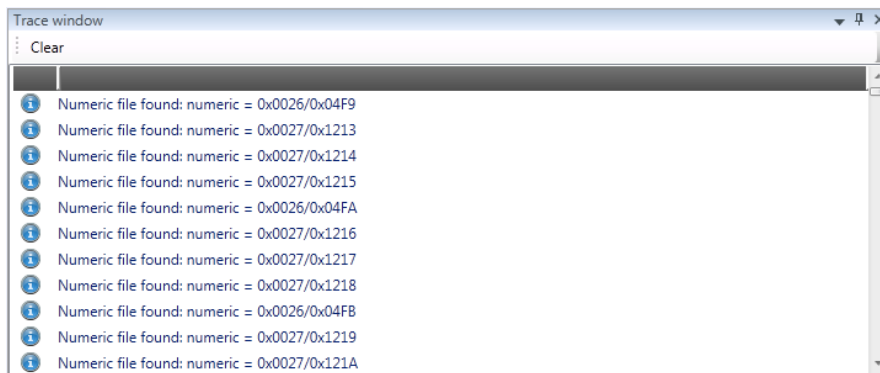
Show Welcome Screen	Displays the <b>Welcome</b> tab. See <a href="#">Welcome tab</a> (page 55).
Trace Window	Show/hide the trace panel at the bottom of the data display area.

### 13.2.1. Viewing the trace window

Show the Trace window at the bottom of the data display area to view a log of the actions performed in your session by you or by UFED Logical Analyzer, such as plug-in activation.

- 1) In the **View** menu, select **Trace Window**.


The Trace window appears below the data display area.



- 2) To clear the log, in the Trace window, click **Clear**.
- 3) To close the Trace window, click **X**.

The Trace window can be hidden or displayed.

- To pin the Trace window open, click **Pin**.

- To unpin the Trace window, click .
- To view the Trace window when hidden, select or mouse over the tab.

### 13.3. Tools menu

Read Data from UFED

Enables data extraction directly to the computer.

Watch List Editor

Opens the Watch List Editor, from where you can create, manage, and run your watch lists. See *Working with watch lists* (page 79).

Malware Scanner

Opens the Malware Scanner sub-menu, from where you can run malware detection on your extraction, and update the signature database.

Translation

Downloads the translation pack from the Internet, installs the translation pack from a file, or displays the supported languages. See *Translating decoded data* (page 93).

TomTom

Opens the TomTom sub-menu, from where you can export the TomTom extraction file and import the returned xml file.

Settings

Access the application settings window. See *Settings* (page 143).

Project Settings

Set unified time zone and case information for each project. See *Setting project settings* (page 169).

## 13.4. Extract menu

### IOS Device Extraction

Starts iOS Device Extraction to perform extractions from iOS devices. See *Performing advanced logical extraction* (page 131).

### Extract GPS/Mass Storage Device

Reads and saves data from GPS and mass storage devices connected to the workstation via USB connection.

## 13.5. Report menu

### Generate Report

Generates a report summary of all information found by the analysis process. See *Generating a report*.

## 13.6. Help menu

### Supported Apps

Lists the supported applications and verified versions for Android and iOS devices.

### Manual

Opens the user manual in PDF format.

### Activate Online Bing Maps

Activates Bing maps so that you can view locations on a map. It requires Internet access and a valid UFED Logical Analyzer license.

### Start UFED Link Analysis Demo

Starts the UFED Link Analysis application

### Show License Details

Displays the current soft or hardware (dongle) license information, and enables you to:

Activate or load a new license (software or dongle)

Display information about previous dongles that were connected to this workstation

Deactivate a soft license

Get direct access via email to Cellebrite support and sales

### Zip Log Files

Zips the log files and opens the folder where the zipped log files are saved.

### Zip Log Files With System Information

Zips the log files and includes detailed information about the operating system, drivers, application data, event logs etc. This information can be used to analyze report cases.

### About

Provides information about the installed UFED Logical Analyzer version.



## A

Activating UFED Logical Analyzer • 19, 27

Adding a new data file type • 154

Adding a new report field • 158, 160

Additional report fields • 123, 157

## B

Bookmarking information • 90

Bookmarking information) • 50

## C

Closing a project • 41

Closing UFED Logical Analyzer • 41

Conversation view • 77

Cover Page • 1

Creating a new entity bookmark • 91

Creating a watch list • 80, 88, 89

## D

Data display area • 53

Data files • 59, 151

Data files filtering methods • 153

Data tabs • 59

Daylight saving time • 149

Deleting a data file type • 156

Deleting a report field • 160

Deleting a watch list • 87

Deleting an entity bookmark • 92

Dongle • 20

## E

Editing a report field • 160

Editing a watch list • 83

Editing an entity bookmark • 92

Editing an existing data file record • 156

Enabling connectivity with Windows Vista • 27

Exporting a watch list • 85

Extract menu • 180

Extracting Data to PC • 32

Extraction from iOS devices • 180

Extraction summary tab • 44, 57

## **F**

File menu • 177

## **G**

General settings • 148

Generating a Report - Report Wizard • 119

Getting started • 29

## **H**

Help menu • 181

## **I**

Image capture • 143

Importing a watch list • 84

Installation and Activation • 9

Installing UFED Logical Analyzer • 10, 12

Introduction • 7

## **L**

Launching UFED Logical Analyzer • 29

Loading a project session • 40

Loading settings • 169

Locating and analyzing information • 69

## **M**

Managing data files settings • 47, 154



Moving the software license • 26

## **N**

Network dongle • 24

New version notification • 19

## **O**

Obtaining a copy of UFED Logical Analyzer • 11

Opening a file for analysis • 30

Orientation to the workspace • 29, 43

## **P**

Performing advanced logical extraction • 131, 132

Performing extractions • 131

Playing video or audio files • 68

Project tree • 44, 58, 59, 90

## **R**

Reference • 177

Report defaults • 123, 161

Report menu • 180

Running a watch list • 88

Running a watch list on particular projects • 88

Running a watch list on your current project • 89

## **S**

Saving a project session • 39

Saving settings • 39, 147, 169

Scanning for malware • 109

screenshots • 143

Searching for information in a data tab • 69

Searching for information in all open projects • 73

Selecting languages • 95

Setting a unified time zone for the project • 170

Setting project settings • 51, 169, 179  
Setting the case information • 123, 173  
Settings • 147, 179  
Shortcuts • 42  
Software installation • 11  
Software license • 21  
System requirements • 10

## **T**

Table view for analyzed data • 66  
Table view for data files • 64  
Text view • 63  
Timeline view • 74  
Tools menu • 179  
Translating decoded data • 93

## **U**

ufdx file • 145, 146  
Updating the signature database (online) • 109, 110  
Updating the signature database from file (offline)  
• 109, 112  
Using the advanced filter • 72  
Using the quick filter • 69

## **V**

View menu • 177  
Viewing image files • 60, 67  
Viewing the trace window • 178

## **W**

Welcome tab • 55, 177  
Working in data tabs • 60

Working in the Project Tree area • 52

Working with Project Analytics • 107

Working with watch lists • 49, 79, 179